Einführung der Gesundheitskarte

Spezifikation der gSMC-KT

Objektsystem

|  |  |
| --- | --- |
| Version: | 3.9.0 |
| Revision: | \main\rel\_online\rel\_ors1\rel\_opb1\11 |
| Stand: | 04.03.2016 |
| Status: | freigegeben |
| Klassifizierung: | öffentlich |
| Referenzierung: | [gemSpec\_gSMC-KT\_ObjSys] |

**Dokumentinformationen**

Änderungen zur Vorversion

* + 1. 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 *persistenPublicKeyList* 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 RC | 04.03.16 |  | zur Freigabe empfohlen | gematik |
| 3.9.0 |  |  | freigegeben | gematik |

**Inhaltsverzeichnis**

[Dokumentinformationen 2](#_Toc503168524)

[Inhaltsverzeichnis 3](#_Toc503168525)

[1 Einordnung des Dokuments 7](#_Toc503168526)

[1.1 Zielsetzung 7](#_Toc503168527)

[1.2 Zielgruppe 7](#_Toc503168528)

[1.3 Geltungsbereich 7](#_Toc503168529)

[1.4 Abgrenzung des Dokuments 8](#_Toc503168530)

[1.5 Methodik 8](#_Toc503168531)

[1.5.1 Nomenklatur 8](#_Toc503168532)

[1.5.2 Verwendung von Schüsselworten 10](#_Toc503168533)

[1.5.3 Komponentenspezifische Anforderungen 10](#_Toc503168534)

[2 Optionen 12](#_Toc503168535)

[2.1 Lange Lebensdauer im Feld 12](#_Toc503168536)

[2.2 Kartenadministration 12](#_Toc503168537)

[3 Lebenszyklus von Karte und Applikation 14](#_Toc503168538)

[4 Anwendungsübergreifende Festlegungen 15](#_Toc503168539)

[4.1 Mindestanzahl logischer Kanäle 15](#_Toc503168540)

[4.2 Kryptobox 15](#_Toc503168541)

[4.3 Optionale Funktionspakete 15](#_Toc503168542)

[4.3.1 Kontaktlose Schnittstelle 15](#_Toc503168543)

[4.3.2 USB-Schnittstelle (optional) 16](#_Toc503168544)

[4.3.3 Option\_PACE\_PCD (optional) 16](#_Toc503168545)

[4.4 Attributstabellen 16](#_Toc503168546)

[4.4.1 Attribute eines Ordners 17](#_Toc503168547)

[4.4.2 Attribute einer Datei (EF) 17](#_Toc503168548)

[4.5 Zugriffsregeln für besondere Kommandos 17](#_Toc503168549)

[4.6 Attributswerte und Personalisierung 18](#_Toc503168550)

[5 Dateisystem der gSMC-KT 19](#_Toc503168551)

[5.1 Attribute des Objektsystems 19](#_Toc503168552)

[5.2 ATR-Kodierung und technische Eigenschaften 20](#_Toc503168553)

[5.3 Allgemeine Struktur 21](#_Toc503168554)

[5.4 Root-Anwendung und Dateien auf MF-Ebene 22](#_Toc503168555)

[5.4.1 MF 22](#_Toc503168556)

[5.4.2 MF / EF.ATR 23](#_Toc503168557)

[5.4.3 MF / EF.DIR 24](#_Toc503168558)

[5.4.4 MF / EF.GDO 25](#_Toc503168559)

[5.4.5 MF / EF.KeyInfo 27](#_Toc503168560)

[5.4.6 MF / EF.Version2 28](#_Toc503168561)

[5.4.7 MF / EF.C.CA\_SMC.CS.E256 29](#_Toc503168562)

[5.4.8 MF / EF.C.CA\_SMC.CS.E384 (Option\_lange\_Lebensdauer\_im\_Feld) 31](#_Toc503168563)

[5.4.9 MF / EF.C.SMC.AUTD\_RPS\_CVC.E256 32](#_Toc503168564)

[5.4.10 MF / EF.C.SMC.AUTD\_RPS\_CVC.E384 (Option\_lange\_Lebensdauer\_im\_Feld) 33](#_Toc503168565)

[5.4.11 MF / PrK.SMC.AUTD\_RPS\_CVC.E256 34](#_Toc503168566)

[5.4.12 MF / PrK.SMC.AUTD\_RPS\_CVC.E384 (Option\_lange\_Lebensdauer\_im\_Feld) 36](#_Toc503168567)

[5.4.13 Sicherheitsanker zum Import von CV-Zertifikaten 37](#_Toc503168568)

[5.4.13.1 MF / PuK.RCA.CS.E256 37](#_Toc503168569)

[5.4.14 Asymmetrische Kartenadministration 39](#_Toc503168570)

[5.4.14.1 MF / PuK.RCA.ADMINCMS.CS.E256 40](#_Toc503168571)

[5.4.15 Symmetrische Kartenadministration 42](#_Toc503168572)

[5.4.15.1 MF / SK.CMS.AES128 42](#_Toc503168573)

[5.4.15.2 MF / SK.CMS.AES256 43](#_Toc503168574)

[5.4.15.3 MF / SK.CUP.AES128 44](#_Toc503168575)

[5.4.15.4 MF / SK.CUP.AES256 45](#_Toc503168576)

[5.5 MF / DF.KT (Kartenterminalanwendung) 46](#_Toc503168577)

[5.5.1 Dateistruktur und Dateiinhalt 46](#_Toc503168578)

[5.5.2 MF / DF.KT / EF.C.SMKT.CA.R2048 48](#_Toc503168579)

[5.5.3 MF / DF.KT / EF.C.SMKT.AUT.R2048 49](#_Toc503168580)

[5.5.4 MF / DF.KT / PrK.SMKT.AUT.R2048 51](#_Toc503168581)

[5.5.5 MF / DF.KT / EF.C.SMKT.CA2.XXXX (Option\_lange\_Lebensdauer\_im\_Feld) 53](#_Toc503168582)

[5.5.6 MF / DF.KT / EF.C.SMKT.AUT2.XXXX (Option\_lange\_Lebensdauer\_im\_Feld) 54](#_Toc503168583)

[5.5.7 MF / DF.KT / PrK.SMKT.AUT2.R2048 (Option\_lange\_Lebensdauer\_im\_Feld) 55](#_Toc503168584)

[5.5.8 MF / DF.KT / PrK.SMKT.AUT.R3072 (Option\_lange\_Lebensdauer\_im\_Feld) 56](#_Toc503168585)

[5.5.9 MF / DF.KT / PrK.SMKT.AUT.E256 (Option\_lange\_Lebensdauer\_im\_Feld) 57](#_Toc503168586)

[5.5.10 MF / DF.KT / PrK.SMKT.AUT.E384 (Option\_lange\_Lebensdauer\_im\_Feld) 58](#_Toc503168587)

[5.6 Laden einer neuen Anwendung oder Anlegen eines EFs nach Ausgabe der gSMC-KT 58](#_Toc503168588)

[6 Anhang A - Verzeichnisse 60](#_Toc503168589)

[6.1 A1 – Abkürzungen 60](#_Toc503168590)

[6.2 A2 – Glossar 60](#_Toc503168591)

[6.3 A3 – Abbildungsverzeichnis 60](#_Toc503168592)

[6.4 A4 – Tabellenverzeichnis 61](#_Toc503168593)

[6.5 A5 – Referenzierte Dokumente 63](#_Toc503168594)

[6.5.1 A5.1 – Dokumente der gematik 63](#_Toc503168595)

[6.5.2 A5.2 – Weitere Dokumente 63](#_Toc503168596)

# 

# Einordnung des Dokuments

## Zielsetzung

* + 1. 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.
    2. 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.
    3. Die Spezifikation behandelt Anwendungen der gSMC-KT unter den folgenden, rein kartenorientierten Gesichtspunkten:
  + Ordnerstruktur,
  + Dateien,
  + Sicherheitsmechanismen wie Zugriffsregeln.
    1. 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.

## Zielgruppe

* + 1. 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.

## Geltungsbereich

* + 1. 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.
    2. **Schutzrechts-/Patentrechtshinweis**
    3. *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*

## Abgrenzung des Dokuments

* + 1. 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.
    2. 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.

## Methodik

### Nomenklatur

* + 1. Dieses Dokument verwendet dieselbe Nomenklatur wie [gemSpec\_COS].

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

* + 1. 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, …).
    2. Der Begriff "Wildcard" wird in diesem Dokument im Sinn eines "beliebigen, herstellerspezifischen Wertes, der nicht anderen Vorgaben widerspricht" verwendet.
    3. 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.
    4. 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.
    5. 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.
    6. 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) |

* + 1. 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 |

* + 1. 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:
    2. 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:
   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.
4. 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.

### Verwendung von Schüsselworten

* + 1. 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
    2. Sie werden im Dokument wie folgt dargestellt:
    3. **⌦ Card-G2-A\_0000 <Titel der Afo>**
    4. Text / Beschreibung
    5. **⌫**
    6. Dabei umfasst die Anforderung sämtliche innerhalb der Textmarken angeführten Inhalte.

### Komponentenspezifische Anforderungen

* + 1. 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 |

# 

# Optionen

* + 1. Dieses Unterkapitel listet Funktionspakete auf, die für eine Zulassung einer gSMC-KT der Generation 2 nicht zwingend erforderlich sind.

## Lange Lebensdauer im Feld

* + 1. **⌦ Card-G2-A\_3018** **Option\_lange\_Lebensdauer\_im\_Feld**
    2. 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.
    3. Die gSMC-KT KANN die Option\_lange\_Lebensdauer\_im\_Feld unterstützen.
    4. **⌫**
    5. **⌦ 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.
3. **⌫**

## Kartenadministration

* + 1. 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.
    2. **⌦ 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

* + - * 1. symmetrische Authentifizierung (SK.CMS und SK.CUP)
        2. 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.

**⌫**

* + 1. **⌦ 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.

* + 1. **⌫**

# Lebenszyklus von Karte und Applikation

* + 1. Diese Spezifikation gilt nicht für die Vorbereitungsphase von Applikationen oder deren Bestandteile. Sie beschreibt lediglich den Zustand des Objektsystems in der Nutzungsphase.
    2. 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.

# 

# Anwendungsübergreifende Festlegungen

* + 1. Zur Umsetzung dieses Kartentyps ist ein Betriebssystem erforderlich, welches folgende Optionen enthält:
  + Unterstützung von mindestens vier logischen Kanälen.
  + Unterstützung der Kryptobox-Funktionalität.

## Mindestanzahl logischer Kanäle

* + 1. **⌦ Card-G2-A\_2475 K\_Initialisierung: Anzahl logischer Kanäle**

Für die Anzahl logischer Kanäle, die von einer gSMC-KT 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 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.
3. **⌫**

## Kryptobox

* + 1. **⌦ Card-G2-A\_2876 K\_gSMC-KT: Kryptobox**
    2. Für das Objektsystem der gSMC-KT MUSS ein COS verwendet werden, das die Kryptobox implementiert hat.
    3. **⌫**

## Optionale Funktionspakete

### Kontaktlose Schnittstelle

* + 1. **⌦ 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.

* + 1. **⌫**

### USB-Schnittstelle (optional)

* + 1. **⌦ 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.

**⌫**

* + 1. **⌦ 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.

**⌫**

### Option\_PACE\_PCD (optional)

* + 1. **⌦ 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.

* + 1. **⌫**

## Attributstabellen

* + 1. **⌦ Card-G2-A\_2469 K\_Initialisierung: Änderung von Zugriffsregeln**

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

* + 1. **⌫**
    2. 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.
    3. Alle Angaben zu Objekten (Ordnern, Dateien, Passwörtern und Schlüsseln) in diesem Dokument beziehen sich ausschließlich auf das Security Environment SE#1.
    4. **⌦ Card-G2-A\_2470 K\_Initialisierung: Verwendung von SE**

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

* + 1. **⌫**
    2. **⌦ 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.

**⌫**

* + 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.

* + 1. **⌫**

### Attribute eines Ordners

* + 1. **⌦ 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.
    1. **⌫**

### Attribute einer Datei (EF)

* + 1. **⌦ 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.

* + 1. **⌫**
    2. **⌦ 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.

* + 1. **⌫**

## Zugriffsregeln für besondere Kommandos

* + 1. Gemäß [gemSpec\_COS] wird festgelegt:
    2. **⌦ 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.

* + 1. **⌫**

## Attributswerte und Personalisierung

* + 1. 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.
    2. 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.
    3. 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.
    4. Die folgende Anforderung ermöglicht herstellerspezifische Personalisierungsprozesse:
    5. **⌦ 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.

* + 1. **⌫**

# Dateisystem der gSMC-KT

* + 1. 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.
    1. **⌦ Card-G2-A\_2477 K\_Personalisierung: weitere Applikationen**

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

* + 1. **⌫**
    2. **⌦ 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.

* + 1. **⌫**

## Attribute des Objektsystems

* + 1. Das Objektsystem der Komponente gSMC-KT enthält gemäß [gemSpec\_COS] folgende Attribute:
    2. **⌦ Card-G2-A\_3273 K\_Initialisierung: Wert des Attributes *root***

Der Wert des Attributes *root* MUSS die Anwendung gemäß Tab\_eGK\_ObjSys\_006 sein.

**⌫**

* + 1. **⌦ 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\_2483entsprechen.

* + 1. **⌫**
    2. **⌦ 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.

* + 1. **⌫**
    2. **⌦ Card-G2-A\_3196 K\_Initialisierung: Inhalt persistent­Public­Key­List**

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

* + 1. **⌫**
    2. **⌦ 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.

* + 1. **⌫**
    2. **⌦ 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.

* + 1. **⌫**
    2. **⌦ 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.

* + 1. **⌫**

## 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.

* + 1. **⌦ 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) |

* + 1. **⌫**
    2. **⌦ 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.

* + 1. **⌫**
    2. **⌦ Card-G2-A\_3027 K\_Personalisierung und K\_Initialisierung: Historical Bytes im ATR**

Das Attribut answerToReset SOLL keine Historical Bytes enthalten.

**⌫**

* + 1. **⌦ Card-G2-A\_2483 K\_Personalisierung und K\_Initialisierung: Vorgaben für Historical Bytes**
    2. Falls answerToReset Historical Bytes enthält, dann MÜSSEN
  1. diese gemäß [ISO7816-4] kodiert sein.
  2. die dort getroffenen Angaben konsistent sein zu Angaben im EF.ATR.
  3. **⌫**

## Allgemeine Struktur

* + 1. Die Abbildung Abb\_gSMC-KT-ObjSys\_001 zeigt die allgemeine Struktur der gSMC-KT.
    2. 

Abbildung 1: Abb\_gSMC-KT-ObjSys\_001 Objektstruktur einer gSMC-KT auf oberster Ebene

## Root-Anwendung und Dateien auf MF-Ebene

### MF

* + 1. Das MF der gSMC-KT ist ein “Application Dedicated File” (siehe [gem­Spec\_COS#8.3.1.3]).
    2. **⌦ 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) |

* + 1. **⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem Ordnerobjekt arbeiten, sind:   
   Activate, Deactivate, Delete, Fingerprint, List Public Key, Load Application, Select, Terminate DF.
2. Da sich weder dieser Ordner noch darüberliegende Ebenen deaktivieren lassen, sind diese Zustände für Objekte im Kapitel 5.4 im Allgemeinen irrelevant.
3. Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kap.5.6

### MF / EF.ATR

* + 1. Die transparente Datei EF.ATR enthält Informationen zur maximalen Größe der APDU sowie zur Identifizierung des Betriebssystems.
    2. **⌦ 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 |  |
| *positionLogicalEndOfFile* | 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) |

* + 1. **⌫**

1. 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.
2. Der Wert des Attributs fileIdentifier ist in [ISO 7816–4] festgelegt.
   * 1. **⌦ Card-G2-A\_3471 K\_Initialisierung: Initialisiertes Attribu*t 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.
  + 1. **⌫**

### MF / EF.DIR

* + 1. 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.
    2. **⌦ 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) |

* + 1. **⌫**

1. 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.
2. Die Werte von fileIdentifier und shortFileIdentifier sind in [ISO 7816–4] festgelegt.
3. Die beiden derzeit definierten Rekords benötigen je 21 Oktette.
4. Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kap. 5.6.

### MF / EF.GDO

* + 1. In EF.GDO wird das Datenobjekt ICCSN gespeichert, das die Kennnummer der Karte enthält.
    2. **⌦ 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 |  |
| *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 | siehe Hinweis (2) |
| Zugriffsregel für logischen LCS „Termination state“ | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (2) |

* + 1. **⌫**

1. 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.
   * 1. Das Attribut body enthält die Seriennummer der Karte. Dabei gilt:
     2. **⌦ 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** |
| *positionLogicalEndOfFile* | ‘000C’ Oktett = 12 Oktett |  |
| *body* | Inhalt gemäß [gemSpec\_Karten\_Fach\_TIP] |  |

* + 1. **⌫**

### MF / EF.KeyInfo

* + 1. Die Datei EF.KeyInfo enthält die Information darüber, welche Datei- und Schlüsselreferenzen aktuell zu verwenden sind und welches Gültigskeitsende sie haben.
    2. **⌦ 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 | | |
| 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 |  |

* + 1. **⌫**

1. 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
2. Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar

### MF / EF.Version2

* + 1. 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
    1. Die konkrete Befüllung ist in [gemSpec\_Karten\_Fach\_TIP] beschrieben.
    2. Elemente, die nach Initialisierung durch Personalisierung oder reine Kartennutzung nicht veränderlich sind, werden in EF.ATR versioniert.
    4. **⌦ 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 |  |
| *positionLogicalEndOfFile* | 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) |

* + 1. **⌫**

1. 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
2. Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kap. 5.6

### MF / EF.C.CA\_SMC.CS.E256

* + 1. 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).
    2. **⌦ Card-G2-A\_2496 K\_Initialisierung: Initialisierte Attribute von MF / EF.C.CA\_SMC.CS.E256**
    3. 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 |  |
| *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 (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) |

* + 1. **⌫**

1. 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.
2. Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap.5.6.
   * 1. **⌦ Card-G2-A\_3455 K\_Personalisierung: Personalisierte Attribute von MF / EF.C.CA\_SMC.CS.E256**
     2. 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** |
| *positionLogicalEndOfFile* | ‘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] |

* + 1. **⌫**

### MF / EF.C.CA\_SMC.CS.E384 (Option\_lange\_Lebensdauer\_im\_Feld)

* + 1. 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).
    2. **⌦ 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 |  |
| *positionLogicalEndOfFile* | ’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 |  |

* + 1. **⌫**

### MF / EF.C.SMC.AUTD\_RPS\_CVC.E256

* + 1. 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.
    2. **⌦ 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) |

* + 1. **⌫**

1. 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.
2. Das Zertifikat enthält die Rolle CHAT = Remote PIN Sender (RPS), d.h. in der Flagliste cvc\_FlagList\_TI ist Flag 54 gesetzt.
3. Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap. 5.6.
   * 1. **⌦ 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].

* + 1. **⌫**
    2. **⌦ 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 |  |

* + 1. **⌫**

### MF / EF.C.SMC.AUTD\_RPS\_CVC.E384 (Option\_lange\_Lebensdauer\_im\_Feld)

* + 1. 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.
    2. **⌦ 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 |  |
| *positionLogicalEndOfFile* | ’0’ |  |
| *flagTransactionMode* | True |  |
| *flagChecksum* | False |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *shareable* | True |  |
| body | undefiniert | wird später nachgeladen |
| Zugriffsregeln | | |
| *accessRules* | identisch zu EF.C.SMC.AUTD\_RPS\_CVC.E256 |  |

* + 1. **⌫**
    2. **⌦ 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].

* + 1. **⌫**

### MF / PrK.SMC.AUTD\_RPS\_CVC.E256

* + 1. 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).
    2. **⌦ 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} |  |
| *accessRulesSession keys* | 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) |

* + 1. **⌫**

1. 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
2. Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap. 5.6.
3. Diese Rolle ist einem Gerät für Stapel- und Komfortsignatur zugewiesen. Dabei wird die PIN.QES des "Remote"-Gerätes dorthin übertragen.
4. Diese Rolle ist einem Remote-PIN-Empfänger zugewiesen.
   * 1. **⌦ 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 |  |

* + 1. **⌫**

### MF / PrK.SMC.AUTD\_RPS\_CVC.E384 (Option\_lange\_Lebensdauer\_im\_Feld)

* + 1. 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).
    2. **⌦ 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 } |  |
| *accessRulesSession keys* | 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 |  |

* + 1. **⌫**

1. 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

### Sicherheitsanker zum Import von CV-Zertifikaten

* + 1. 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.

#### MF / PuK.RCA.CS.E256

* + 1. 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).
    2. **⌦ 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 | * OIDflags = 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) |

* + 1. **⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem öffentlichen Signaturprüfobjekt arbeiten, sind: PSO Verify Certificate, Terminate.
2. Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap. 5.6.
3. 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.
   * 1. **⌦ 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 |  |

* + 1. **⌫**

### Asymmetrische Kartenadministration

* + 1. Die hier beschriebene optionale Variante der Administration der gSMC-KT betrifft ein Administrationssystem (i.A. ein Kartenmanagementsystem (CMS)) zur Administration der gSMC-KT.
    2. 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.
    3. 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.
    4. 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. Bei der Personalisierung sind nur die Schlüssel zu personalisieren, die tatsächlich benötigt werden.

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

* + 1. 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.
    2. **⌦ Card-G2-A\_3028 K\_Initialisierung: Initialisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256**
    3. 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 | * OIDflags = 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 |  |

* + 1. **⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem öffentlichen Signaturprüfobjekt arbeiten, sind:   
   Activate, Deactivate, Delete, PSO Verify Certificate, Terminate
2. 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.
3. Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap.5.6.
   * 1. **⌦ Card-G2-A\_3458 K\_Personalisierung: Personalisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256**
     2. 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.
     3. 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 |  |

* + 1. **⌫**

### Symmetrische Kartenadministration

* + 1. Die hier beschriebene optionale Variante der Administration einer gSMC-KT betrifft ein Administrationssystem (i.A. ein Kartenmanagementsystem (CMS)) zur Administration der gSMC-KT.
    2. 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.
    3. Voraussetzung für den Aufbau mittels symmetrischer Verfahren ist, dass sowohl die zu administrierende Karte, als auch das administrierende System über denselben symmetrischen Schlüssel verfügen.
    4. Während die Schlüssel auf Smartcards typischerweise kartenindividuell sind, ist es denkbar, dass mit einem Schlüssel eines administrierenden Systems genau eine, oder mehrere oder alle Smartcards administriert werden. Das Sicherheitskonzept des administrierenden Systems erscheint die geeignete Stelle zu sein um eine Variante auszuwählen.

#### MF / SK.CMS.AES128

* + 1. SK.CMS.AES128 (optional) ist der geheime Schlüssel für die Durchführung des SMC-KT / CMS-Authentisie­rungs­verfahrens mit Aufbau eines Trusted Channel.
    2. **⌦ 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 |  |

* + 1. **⌫**

1. 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.
2. Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap. 5.6.
   * 1. **⌦ 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] |  |

* + 1. **⌫**

#### MF / SK.CMS.AES256

* + 1. SK.CMS.AES256 (optional) ist der geheime Schlüssel für die Durchführung des SMC-KT/CMS-Authentisierungsverfahrens mit Aufbau eines Trusted Channel.
    2. **⌦ 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 |  |

* + 1. **⌫**

1. 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.
   * 1. **⌦ 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] |  |

* + 1. **⌫**

#### MF / SK.CUP.AES128

* + 1. Dieser AES-Schlüssel mit 128 bit Schlüssellänge wird benötigt, um dem CUPS administrative Zugriffe auf die gSMC-KT bezüglich der Zertifikate zu erlauben.
    2. **⌦ 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 |  |

* + 1. **⌫**
    2. **⌦ 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] |  |

* + 1. **⌫**

#### MF / SK.CUP.AES256

* + 1. Dieser AES-Schlüssel mit 256 bit Schlüssellänge wird benötigt, um dem CUPS administrative Zugriffe auf die gSMC-KT bezüglich der Zertifikate zu erlauben.
    2. **⌦ 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 |  |

* + 1. **⌫**
    2. **⌦ 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] |  |

* + 1. **⌫**

## MF / DF.KT (Kartenterminalanwendung)

### Dateistruktur und Dateiinhalt

* + 1. DF.KT wird verwendet für:
  + die Authentisierung zur Anbindung des Kartenterminals an einen bestimmten Konnektor.
    1. Die folgende Abbildung zeigt die Dateistruktur von DF.KT



Abbildung 2: Abb\_gSMC-KT-ObjSys\_002 Dateistruktur von DF.KT

* + 1. 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.
    2. **⌦ 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 |  |

* + 1. **⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem Ordnerobjekt arbeiten, sind:   
   Activate, Deactivate, Delete, Fingerprint, List Public Key, Load Application, Select, Terminate DF.
2. 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.
3. Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kap. 5.6.

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

* + 1. 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.
    2. **⌦ 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 |  |
| *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 (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 |  |

* + 1. **⌫**

1. 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.
2. 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.
3. Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap. 5.6.
   * 1. **⌦ 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** |
| ***positionLogicalEndOfFile*** | Zahl der tatsächlich belegten Oktette |  |
| ***body*** | C.SMKT.CA.R2048 gemäß [gemSpec\_PKI] |  |

* + 1. **⌫**

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

* + 1. **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.
    2. 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.
    3. **⌦ 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 |  |
| *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 (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 |  |

* + 1. **⌫**

1. 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.
2. 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.
3. Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.6.
   * 1. **⌦ 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 |  |

* + 1. **⌫**

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

* + 1. PrK.SMKT.AUT.R2048 ist der private Authentisierungsschlüssel zur Anbindung des Kartenterminals an einen bestimmten Konnektor.
    2. **⌦ 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 | herstellerspezifisch ist eine der beiden Varianten erlaubt |
| AUT\_CMS OR AUT\_CUP |
| 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 | herstellerspezifisch ist eine der beiden Varianten erlaubt |
| AUT\_CMS OR AUT\_CUP |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Termination state“ | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | NEVER |  |

* + 1. **⌫**

1. 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
2. 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.
3. Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap. 5.6.
   * 1. **⌦ 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 |  |

* + 1. **⌫**

### MF / DF.KT / EF.C.SMKT.CA2.XXXX (Option\_lange\_Lebensdauer\_im\_Feld)

* + 1. 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.
    2. **⌦ 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 |  |
| *positionLogicalEndOfFile* | ’0’ | wird später nachgeladen |
| *flagTransactionMode* | 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 |  |

* + 1. **⌫**

1. 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.
2. Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 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.

* + 1. **⌦ 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 |  |
| *positionLogicalEndOfFile* | ’0’ | wird später nachgeladen |
| *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 |  |

* + 1. **⌫**

1. 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.

### MF / DF.KT / PrK.SMKT.AUT2.R2048 (Option\_lange\_Lebensdauer\_im\_Feld)

* + 1. 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.
    2. **⌦ 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 |  |

* + 1. **⌫**

1. 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

### MF / DF.KT / PrK.SMKT.AUT.R3072 (Option\_lange\_Lebensdauer\_im\_Feld)

* + 1. PrK.SMKT.AUT.R3072 ist der private Authentisierungsschlüssel für die Kryptographie mit RSA zur Anbindung des Kartenterminals an einen bestimmten Konnektor.
    2. **⌦ 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 |  |

* + 1. **⌫**

1. 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

### MF / DF.KT / PrK.SMKT.AUT.E256 (Option\_lange\_Lebensdauer\_im\_Feld)

* + 1. PrK.SMKT.AUT.E384 ist der private Authentisierungsschlüssel für die Kryptographie mit mit elliptischen Kurven zur Anbindung des Kartenterminals an einen bestimmten Konnektor.
    2. **⌦ 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 |  |

* + 1. **⌫**

1. 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
2. Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap. 5.6.

### MF / DF.KT / PrK.SMKT.AUT.E384 (Option\_lange\_Lebensdauer\_im\_Feld)

* + 1. PrK.SMKT.AUT.E384 ist der private Authentisierungsschlüssel für die Kryptographie mit mit elliptischen Kurven zur Anbindung des Kartenterminals an einen bestimmten Konnektor.
    2. **⌦ 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 |  |

* + 1. **⌫**

1. 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

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

* + 1. 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.
    2. 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

* + 1. Das Projektglossar wird als eigenständiges Dokument zur Verfügung gestellt.

## A3 – Abbildungsverzeichnis

[Abbildung 1: Abb\_gSMC-KT-ObjSys\_001 Objektstruktur einer gSMC-KT auf oberster Ebene 20](#_Toc458095279)

[Abbildung 2: Abb\_gSMC-KT-ObjSys\_002 Dateistruktur von DF.KT 44](#_Toc458095280)

## A4 – Tabellenverzeichnis

[Tabelle 1: Tab\_gSMC-KT\_ObjSys\_001 Liste der Komponenten, an welche dieses Dokument Anforderungen stellt 10](#_Toc458095236)

[Tabelle 2: Tab\_gSMC-KT\_ObjSys\_002 ATR-Kodierung 19](#_Toc458095237)

[Tabelle 3: Tab\_gSMC-KT\_ObjSys\_004 Initialisierte Attribute von MF 21](#_Toc458095238)

[Tabelle 4: Tab\_gSMC-KT\_ObjSys\_005 Initialisierte Attribute von MF / EF.ATR 21](#_Toc458095239)

[Tabelle 5: Tab\_gSMC-KT\_ObjSys\_012 Initialisierte Attribute von MF / EF.DIR 23](#_Toc458095240)

[Tabelle 6: Tab\_gSMC-KT\_ObjSys\_013 Initialisierte Attribute von MF / EF.GDO 24](#_Toc458095241)

[Tabelle 7: Tab\_gSMC-KT\_ObjSys\_060 Personalisierte Attribute von MF / EF.GDO 25](#_Toc458095242)

[Tabelle 8: Tab\_gSMC-KT\_ObjSys\_059 Initialisierte Attribute von MF / EF.KeyInfo 25](#_Toc458095243)

[Tabelle 9: Tab\_gSMC-KT\_ObjSys\_014 Initialisierte Attribute von MF / EF.Version2 26](#_Toc458095244)

[Tabelle 10: Tab\_gSMC-KT\_ObjSys\_007 Initialisierte Attribute von MF / EF.C.CA\_SMC.CS.E256 28](#_Toc458095245)

[Tabelle 11: Tab\_gSMC-KT\_ObjSys\_035 Personalisierte Attribute von MF / EF.C.CA\_SMC.CS.E256 29](#_Toc458095246)

[Tabelle 12: Tab\_gSMC-KT\_ObjSys\_008 Initialisierte Attribute von MF / EF.C.CA\_SMC.CS.E384 29](#_Toc458095247)

[Tabelle 13: Tab\_gSMC-KT\_ObjSys\_010 Initialisierte Attribute von MF / EF.C.SMC.AUTD\_RPS\_CVC.E256 30](#_Toc458095248)

[Tabelle 14: Tab\_gSMC-KT\_ObjSys\_037 Personalisierte Attribute von MF / EF.C.SMC.AUTD\_RPS\_CVC.E256 31](#_Toc458095249)

[Tabelle 15: Tab\_gSMC-KT-ObjSys\_011 Initialisierte Attribute von MF / EF.C.SMC.AUTD\_RPS\_CVC.E384 32](#_Toc458095250)

[Tabelle 16: Tab\_gSMC-KT\_ObjSys\_016 Initialisierte Attribute von MF / PrK.SMC.AUTD\_RPS\_CVC.E256 32](#_Toc458095251)

[Tabelle 17: Tab\_gSMC-KT\_ObjSys\_042 Personalisierte Attribute von MF / PrK.SMC.AUTD\_RPS\_CVC.E256 34](#_Toc458095252)

[Tabelle 18: Tab\_gSMC-KT\_ObjSys\_017 Initialisierte Attribute von MF / PrK.SMC.AUTD\_RPS\_CVC.E384 34](#_Toc458095253)

[Tabelle 19: Tab\_gSMC-KT\_ObjSys\_019 Initialisierte Attribute von MF / PuK.RCA.CS.E256 35](#_Toc458095254)

[Tabelle 20: Tab\_gSMC-KT\_ObjSys\_058 Personalisierte Attribute von MF / PuK.RCA.CS.E256 für Testkarten 37](#_Toc458095255)

[Tabelle 21: Tab\_gSMC-KT\_ObjSys\_031 Initialisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256 38](#_Toc458095256)

[Tabelle 22: Tab\_gSMC-KT\_ObjSys\_044 Personalisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256 39](#_Toc458095257)

[Tabelle 23: Tab\_gSMC-KT\_ObjSys\_023 Initialisierte Attribute von MF / SK.CMS.AES128 40](#_Toc458095258)

[Tabelle 24: Tab\_gSMC-KT\_ObjSys\_045 Personalisierte Attribute von MF / SK.CMS.AES128 41](#_Toc458095259)

[Tabelle 25: Tab\_gSMC-KT\_ObjSys\_024 Initialisierte Attribute von MF / SK.CMS.AES256 41](#_Toc458095260)

[Tabelle 26: Tab\_gSMC-KT\_ObjSys\_046 Personalisierte Attribute von MF / SK.CMS.AES256 42](#_Toc458095261)

[Tabelle 27: Tab\_gSMC-KT\_ObjSys\_054 Initialisierte Attribute von MF / SK.CUP.AES128 42](#_Toc458095262)

[Tabelle 28: Tab\_gSMC-KT\_ObjSys\_055 Personalisierte Attribute von MF / SK.CUP.AES128 43](#_Toc458095263)

[Tabelle 29: Tab\_gSMC-KT\_ObjSys\_056 Initialisierte Attribute von MF / SK.CUP.AES256 43](#_Toc458095264)

[Tabelle 30: Tab\_gSMC-KT\_ObjSys\_057 Personalisierte Attribute von MF / SK.CUP.AES256 43](#_Toc458095265)

[Tabelle 31: Tab\_gSMC-KT\_ObjSys\_025 Initialisierte Attribute von MF / DF.KT 44](#_Toc458095266)

[Tabelle 32: Tab\_gSMC-KT\_ObjSys\_026 Initialisierte Attribute von MF / DF.KT / EF.C.SMKT.CA.R2048 45](#_Toc458095267)

[Tabelle 33: Tab\_gSMC-KT\_ObjSys\_047 Personalisierte Attribute von MF / DF.KT / EF.C.SMKT.CA.R2048 47](#_Toc458095268)

[Tabelle 34: Tab\_gSMC-KT\_ObjSys\_027 Initialisierte Attribute von MF / DF.KT / EF.C.SMKT.AUT.R2048 47](#_Toc458095269)

[Tabelle 35: Tab\_gSMC-KT\_ObjSys\_049 Personalisierte Attribute von MF / DF.KT / EF.C.SMKT.AUT.R2048 48](#_Toc458095270)

[Tabelle 36: Tab\_gSMC-KT\_ObjSys\_028 Initialisierte Attribute von MF / DF.KT / PrK.SMKT.AUT.R2048 49](#_Toc458095271)

[Tabelle 37: Tab\_gSMC-KT\_ObjSys\_051 Personalisierte Attribute von MF / DF.KT / PrK.SMKT.AUT.R2048 50](#_Toc458095272)

[Tabelle 38: Tab\_gSMC-KT\_ObjSys\_032 Initialisierte Attribute von MF / DF.KT / EF.C.SMKT.CA2.XXXX 50](#_Toc458095273)

[Tabelle 39: Tab\_gSMC-KT\_ObjSys\_033 Initialisierte Attribute von MF / DF.KT / EF.C.SMKT.AUT.XXXX 52](#_Toc458095274)

[Tabelle 40: Tab\_gSMC-KT\_ObjSys\_061 Initialisierte Attribute von MF / DF.KT / PrK.SMKT.AUT2.R2048 52](#_Toc458095275)

[Tabelle 41: Tab\_gSMC-KT\_ObjSys\_029 Initialisierte Attribute von MF / DF.KT / PrK.SMKT.AUT.R3072 53](#_Toc458095276)

[Tabelle 42: Tab\_gSMC-KT\_ObjSys\_062 Initialisierte Attribute von MF / DF.KT / PrK.SMKT.AUT.E256 54](#_Toc458095277)

[Tabelle 43: Tab\_gSMC-KT\_ObjSys\_030 Initialisierte Attribute von MF / DF.KT / PrK.SMKT.AUT.E384 55](#_Toc458095278)

## A5 – Referenzierte Dokumente

### A5.1 – Dokumente der gematik

* + 1. 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 – 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> |