1. Einführung der Gesundheitskarte

Spezifikation der gSMC-K Objektsystem

|  |  |
| --- | --- |
| Version: | 3.10.0 |
| Revision: | \main\rel\_online\rel\_ors1\rel\_opb1\26 |
| Stand: | 28.10.2016 |
| Status: | freigegeben |
| Klassifizierung: | öffentlich |
| Referenzierung: | [gemSpec\_gSMC-K\_ObjSys] |

**Dokumentinformationen**

Änderung 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** |
| --- | --- | --- | --- | --- |
| 2.9.18 | 06.06.12 |  | zur Abstimmung freigegeben | gematik |
| 3.0.0 | 24.08.12 |  | Einfügen von EF.EnvironmentalSettings | gematik |
| 3.1.0 | 17.01.13 |  | Harmonisierung mit der Struktur der anderen ObjSys-Spezifikationen | gematik |
| 3.2.0 RC | 23.10.13 |  | redaktionelle Korrekturen, Fehlerkorrekturen, AFO zu *persistenPublicKeyList* hinzugefügt, Attribut shareable wurde für alle Ordner und Dateien hinzugefügt, Ändern der Flaglist-Darstellung, Fehlerkorrekturen gemäß Kommentaren | gematik |
| 3.3.0 RC | 19.12.13 |  | Zuordnung der AFOs zu Initialisierung und Personalisierung, Überarbeitung der Struktur, Einfügen von EF.KeyInfo, Modifizieren von EF.ATR, EF.DIR und EF.Version, Modifizieren von EF.GDO, Kommentare wurden eingearbeitet | gematik |
| 3.4.0 | 21.02.14 |  | Einfügen einer Liste offener Punkte, Änderungen aus Kommentarliste TSI, 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, Einfügen Schlüssel und Zertifikate für CVC-Admin, Einfügen Option\_Erweiterung\_herstellerspezifische\_Schlüssel\_01 | gematik |
| 3.8.0 | 17.07.15 |  | Folgende Errata eingearbeitet:  R.1.4.1, R1.4.2, R1.4.3, R1.4.5 | Technik / SPE |
| 3.9.0 | 24.08.16 |  | Anpassungen zum Online-Produktivbetrieb (Stufe 1) | gematik |
|  |  |  | Einarbeitung Änderungsliste |  |
| 3.10.0 | 28.10.16 |  | freigegeben | gematik |

Inhaltsverzeichnis

[1 Einordnung des Dokumentes 8](#_Toc503168896)

[1.1 Zielsetzung 8](#_Toc503168897)

[1.2 Zielgruppe 8](#_Toc503168898)

[1.3 Geltungsbereich 8](#_Toc503168899)

[1.4 Abgrenzung des Dokuments 9](#_Toc503168900)

[1.5 Methodik 9](#_Toc503168901)

[1.5.1 Nomenklatur 9](#_Toc503168902)

[1.5.2 Verwendung von Schüsselworten 11](#_Toc503168903)

[1.5.3 Komponentenspezifische Anforderungen 11](#_Toc503168904)

[2 Optionen 12](#_Toc503168905)

[2.1 Option\_Erstellung\_von\_Testkarten 12](#_Toc503168906)

[2.2 Option\_Erweiterung\_herstellerspezifische\_Schlüssel\_01 12](#_Toc503168907)

[3 Lebenszyklus von Karte und Applikation 13](#_Toc503168908)

[4 Anwendungsübergreifende Festlegungen 14](#_Toc503168909)

[4.1 Mindestanzahl logischer Kanäle 14](#_Toc503168910)

[4.2 Kryptobox 14](#_Toc503168911)

[4.3 Optionale Funktionspakete 14](#_Toc503168912)

[4.3.1 Kontaktlose Schnittstelle 14](#_Toc503168913)

[4.3.2 USB-Schnittstelle (optional) 15](#_Toc503168914)

[4.4 Attributstabellen 15](#_Toc503168915)

[4.4.1 Attribute eines Ordners 15](#_Toc503168916)

[4.4.2 Attribute einer Datei (EF) 16](#_Toc503168917)

[4.5 Zugriffsregeln für besondere Kommandos 16](#_Toc503168918)

[4.6 TransportStatus für Passwortobjekte 17](#_Toc503168919)

[4.7 Attributswerte und Personalisierung 17](#_Toc503168920)

[4.8 Kartenadministration 18](#_Toc503168921)

[5 Dateisystem der gSMC-K 19](#_Toc503168922)

[5.1 Attribute des Objektsystems 19](#_Toc503168923)

[5.1.1 ATR-Kodierung und technische Eigenschaften ATR-Kodierung 20](#_Toc503168924)

[5.2 Allgemeine Struktur 21](#_Toc503168925)

[5.3 Root-Anwendung und Dateien auf MF-Ebene 22](#_Toc503168926)

[5.3.1 MF 22](#_Toc503168927)

[5.3.2 MF / EF.ATR 23](#_Toc503168928)

[5.3.3 MF / EF.DIR 24](#_Toc503168929)

[5.3.4 MF / EF.EnvironmentSettings 26](#_Toc503168930)

[5.3.5 MF / EF.GDO 27](#_Toc503168931)

[5.3.6 MF / EF.KeyInfo 28](#_Toc503168932)

[5.3.7 MF / EF.Version2 29](#_Toc503168933)

[5.3.8 MF / EF.C.CA\_SAK.CS.E256 30](#_Toc503168934)

[5.3.9 MF / EF.C.CA\_SAK.CS.E384 32](#_Toc503168935)

[5.3.10 MF / EF.PuK.RCA.CS.R2048 33](#_Toc503168936)

[5.3.11 MF / EF.C.RCA.CS.E256 34](#_Toc503168937)

[5.3.12 MF / EF.C.SMC.AUT\_CVC.E256 36](#_Toc503168938)

[5.3.13 MF / EF.C.SMC.AUT\_CVC.E384 37](#_Toc503168939)

[5.3.14 MF / PIN.AK 38](#_Toc503168940)

[5.3.15 MF / PIN.NK 40](#_Toc503168941)

[5.3.16 MF / PIN.Pers 42](#_Toc503168942)

[5.3.17 MF / PIN.SAK 43](#_Toc503168943)

[5.3.18 MF / PrK.SMC.AUT\_CVC.E256 45](#_Toc503168944)

[5.3.19 MF / PrK.SMC.AUT\_CVC.E384 47](#_Toc503168945)

[5.3.20 Herstellerspezifische Schlüssel 48](#_Toc503168946)

[5.3.20.1 MF / PrK.KONN.AUT.R2048 48](#_Toc503168947)

[5.3.20.2 MF / PrK.KONN.AUT2.R2048 50](#_Toc503168948)

[5.3.20.3 MF / PrK.KONN.AUT.R3072 51](#_Toc503168949)

[5.3.20.4 MF / PrK.KONN.AUT.E256 52](#_Toc503168950)

[5.3.20.5 MF / PrK.KONN.AUT.E384 53](#_Toc503168951)

[5.3.20.6 MF / PrK.KONN.ENC.R2048 (Option\_Erweiterung\_herstellerspezifische\_Schlüssel\_01) 54](#_Toc503168952)

[5.3.20.7 MF / PrK.KONN.ENC2.R2048 (Option\_Erweiterung\_herstellerspezifische\_Schlüssel\_01) 55](#_Toc503168953)

[5.3.20.8 MF / PrK.KONN.ENC.R3072 (Option\_Erweiterung\_herstellerspezifische\_Schlüssel\_01) 56](#_Toc503168954)

[5.3.20.9 MF / PrK.KONN.TLS.R2048 (Option\_Erweiterung\_herstellerspezifische\_Schlüssel\_01) 57](#_Toc503168955)

[5.3.20.10 MF / PrK.KONN.TLS2.R2048 (Option\_Erweiterung\_herstellerspezifische\_Schlüssel\_01) 59](#_Toc503168956)

[5.3.20.11 MF / PrK.KONN.TLS.R3072 (Option\_Erweiterung\_herstellerspezifische\_Schlüssel\_01) 60](#_Toc503168957)

[5.3.20.12 MF / EF.PuK.KONN.SIG.R4096 (Option\_Erweiterung\_herstellerspezifische\_Schlüssel\_01) 61](#_Toc503168958)

[5.3.20.13 MF / PrK.SDS.R2048 (Option\_Erweiterung\_herstellerspezifische\_Schlüssel\_01) 62](#_Toc503168959)

[5.3.20.14 MF / PrK.SDS2.R2048 (Option\_Erweiterung\_herstellerspezifische\_Schlüssel\_01) 64](#_Toc503168960)

[5.3.20.15 MF / PrK.SDS.R3072 (Option\_Erweiterung\_herstellerspezifische\_Schlüssel\_01) 65](#_Toc503168961)

[5.3.20.16 MF / PrK.GP.R2048 66](#_Toc503168962)

[5.3.20.17 MF / PuK.GP.R2048 67](#_Toc503168963)

[5.3.20.18 MF / PrK.GP2.R2048 69](#_Toc503168964)

[5.3.20.19 MF / PrK.GP.R3072 69](#_Toc503168965)

[5.3.20.20 MF / PrK.GP.E256 70](#_Toc503168966)

[5.3.20.21 MF / PrK.GP.E384 71](#_Toc503168967)

[5.3.21 Sicherheitsanker zum Import von CV-Zertifikaten 72](#_Toc503168968)

[5.3.21.1 MF / PuK.RCA.CS.E256 72](#_Toc503168969)

[5.3.22 Asymmetrische Kartenadministration 74](#_Toc503168970)

[5.3.22.1 MF / PuK.RCA.ADMINCMS.CS.E256 74](#_Toc503168971)

[5.3.23 Symmetrische Kartenadministration 76](#_Toc503168972)

[5.3.23.1 MF /. SK.CMS.AES128 76](#_Toc503168973)

[5.3.23.2 MF / SK.CMS.AES256 78](#_Toc503168974)

[5.3.23.3 MF / SK.CUP.AES128 79](#_Toc503168975)

[5.3.23.4 MF / SK.CUP.AES256 80](#_Toc503168976)

[5.4 MF / DF.AK 81](#_Toc503168977)

[5.4.1 MF /DF.AK/ EF.C.AK.AUT.R2048 83](#_Toc503168978)

[5.4.2 MF / DF.AK / PrK.AK.AUT.R2048 84](#_Toc503168979)

[5.4.3 MF /DF.AK/ EF.C.AK.AUT2.XXXX 86](#_Toc503168980)

[5.4.4 MF / DF.AK / PrK.AK.AUT2.R2048 87](#_Toc503168981)

[5.4.5 MF / DF.AK / PrK.AK.AUT.R3072 88](#_Toc503168982)

[5.4.6 MF / DF.AK / PrK.AK.AUT.E256 89](#_Toc503168983)

[5.4.7 MF / DF.AK / PrK.AK.AUT.E384 90](#_Toc503168984)

[5.4.8 MF / DF.AK / PrK.AK.CA\_PS.R2048 91](#_Toc503168985)

[5.4.9 MF / DF.AK / PrK.AK.CA\_PS2.R2048 92](#_Toc503168986)

[5.4.10 MF / DF.AK / PrK.AK.CA\_PS.R3072 93](#_Toc503168987)

[5.4.11 MF / DF.AK / PrK.AK.CA\_PS.E256 94](#_Toc503168988)

[5.4.12 MF / DF.AK / PrK.AK.CA\_PS.E384 95](#_Toc503168989)

[5.5 MF / DF.NK 95](#_Toc503168990)

[5.5.1 MF / DF.NK / EF.ActKey 97](#_Toc503168991)

[5.5.2 MF / DF.NK / EF.CardInfo 98](#_Toc503168992)

[5.5.3 MF / DF.NK / EF.CFSMACKey 99](#_Toc503168993)

[5.5.4 MF / DF.NK / EF.ConfigUser 100](#_Toc503168994)

[5.5.5 MF /DF.NK/ EF.C.NK.VPN.R2048 101](#_Toc503168995)

[5.5.6 MF / DF.NK / PrK.NK.VPN.R2048 102](#_Toc503168996)

[5.5.7 MF /DF.NK/ EF.C.NK.VPN2.XXXX 104](#_Toc503168997)

[5.5.8 MF / DF.NK / PrK.NK.VPN2.R2048 105](#_Toc503168998)

[5.5.9 MF / DF.NK / PrK.NK.VPN.R3072 106](#_Toc503168999)

[5.5.10 MF / DF.NK / PrK.NK.VPN.E256 106](#_Toc503169000)

[5.5.11 MF / DF.NK / PrK.NK.VPN.E384 107](#_Toc503169001)

[5.5.12 MF / DF.NK / PrK.CFS.R2048 108](#_Toc503169002)

[5.5.13 MF / DF.NK / PuK.CFS.R2048 109](#_Toc503169003)

[5.5.14 MF / DF.NK / PrK.CFS2.R2048 110](#_Toc503169004)

[5.5.15 MF / DF.NK / PrK.CFS.R3072 111](#_Toc503169005)

[5.5.16 MF / DF.NK / PrK.CFS.E256 112](#_Toc503169006)

[5.5.17 MF / DF.NK / PrK.CFS.E384 113](#_Toc503169007)

[5.6 MF / DF.SAK 114](#_Toc503169008)

[5.6.1 MF / DF.SAK / EF.C.SAK.AUT.R2048 116](#_Toc503169009)

[5.6.2 MF / DF.SAK / PrK.SAK.AUT.R2048 117](#_Toc503169010)

[5.6.3 MF / DF.SAK / EF.C.SAK.AUT2.XXXX 119](#_Toc503169011)

[5.6.4 MF / DF.SAK / PrK.SAK.AUT2.R2048 120](#_Toc503169012)

[5.6.5 MF / DF.SAK / PrK.SAK.AUT.R3072 121](#_Toc503169013)

[5.6.6 MF / DF.SAK / PrK.SAK.AUT.E256 122](#_Toc503169014)

[5.6.7 MF / DF.SAK / PrK.SAK.AUT.E384 122](#_Toc503169015)

[5.6.8 MF / DF.SAK / EF.C.SAK.AUTD\_CVC.E256 123](#_Toc503169016)

[5.6.9 MF / DF.SAK / PrK.SAK.AUTD\_CVC.E256 124](#_Toc503169017)

[5.6.10 MF / DF.SAK / EF.C.SAK.AUTD\_CVC.E384 126](#_Toc503169018)

[5.6.11 MF / DF.SAK / PrK.SAK.AUTD\_CVC.E384 127](#_Toc503169019)

[5.6.12 MF / DF.SAK / PrK.SAK.CA\_xTV.R2048 127](#_Toc503169020)

[5.6.13 MF / DF.SAK / PrK.SAK.CA\_xTV2.R2048 129](#_Toc503169021)

[5.6.14 MF / DF.SAK / PrK.SAK.CA\_xTV.R3072 130](#_Toc503169022)

[5.6.15 MF / DF.SAK / PrK.SAK.CA\_xTV.E256 130](#_Toc503169023)

[5.6.16 MF / DF.SAK / PrK.SAK.CA\_xTV.E384 131](#_Toc503169024)

[5.6.17 MF / DF.SAK / PrK.SAK.SIG.R2048 132](#_Toc503169025)

[5.6.18 MF / DF.SAK / PrK.SAK.SIG2.R2048 133](#_Toc503169026)

[5.6.19 MF / DF.SAK / PrK.SAK.SIG.R3072 134](#_Toc503169027)

[5.6.20 MF / DF.SAK / PrK.SAK.SIG.E256 135](#_Toc503169028)

[5.6.21 MF / DF.SAK / PrK.SAK.SIG.E384 136](#_Toc503169029)

[5.7 MF / DF.Sicherheitsanker 137](#_Toc503169030)

[5.7.1 MF / DF.Sicherheitsanker / EF.C.BNetzA.RCA 138](#_Toc503169031)

[5.7.2 MF / DF.Sicherheitsanker / EF.C.TSL.CA\_1 139](#_Toc503169032)

[5.7.3 MF / DF.Sicherheitsanker / EF.C.TSL.CA\_2 141](#_Toc503169033)

[5.7.4 MF/DF.Sicherheitsanker / PIN.BNetzA\_RCA 142](#_Toc503169034)

[5.7.5 MF/DF.Sicherheitsanker / PIN.TSL\_CA 144](#_Toc503169035)

[5.8 Zusätzliche Applikationen und Dateien 146](#_Toc503169036)

[5.9 EF.GeneralPurpose (kann nach Ausgabe der gSMC-K nachgeladen werden) 147](#_Toc503169037)

[5.10 Laden einer neuen Anwendung oder Anlegen eines EFs oder Sperren von Schlüsseln nach Ausgabe der gSMC-K 148](#_Toc503169038)

[6 Anhang A - Verzeichnisse 149](#_Toc503169039)

[6.1 A1 – Abkürzungen 149](#_Toc503169040)

[6.2 A2 – Glossar 149](#_Toc503169041)

[6.3 A3 – Abbildungsverzeichnis 150](#_Toc503169042)

[6.4 A4 – Tabellenverzeichnis 150](#_Toc503169043)

[6.5 A5 – Referenzierte Dokumente 156](#_Toc503169044)

[6.5.1 A5.1 – Dokumente der gematik 156](#_Toc503169045)

[6.5.2 A5.2 – Weitere Dokumente 156](#_Toc503169046)

# Einordnung des Dokumentes

## Zielsetzung

* + 1. Dieses Dokument beschreibt die Kartenschnittstelle der gerätespezifischen Security Module Card Typ K (gSMC-K) zum Einsatz in Konnektoren.
    2. Die Spezifikation beinhaltet Anwendungen der gSMC-K 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 Schlüsselobjekte durchzuführen etc. Die Semantik und die Syntax der Inhalte in den Datencontainern ist dagegen nicht Gegenstand dieses Dokumentes.

## Zielgruppe

* + 1. Das Dokument richtet sich an Hersteller von Chipkartenbetriebssystemen und an Anwendungsprogrammierer, die unmittelbar mit der gSMC-K kommunizieren, wie etwa Softwareentwickler für Konnektoren.
    2. Zudem richtet es sich an die Produzenten einer gSMC-K, welche die gSMC-K konfigurieren und personalisieren.

## Geltungsbereich

* + 1. Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren An­wendung in Zulassungsverfahren wird durch die gematik GmbH in gesonderten Do­ku­menten (z. B. Dokumentenlandkarte, Produkttypsteckbrief, Leistungsbeschreibung) fest­gelegt und bekannt gegeben.
    2. Der Inhalt des Dokumentes ist verbindlich für die Erstellung von chipkartenbasierten Sicherheitsmodulen gSMC-K, die in Konnektoren zur Anwendung kommen.
    3. **Schutzrechts-/Patentrechtshinweis**
    4. *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. Das Dokument [gemSpec\_COS] beschreibt die Funktionalität eines eGK/HBA/SMC-Betriebssystems, ohne konkret eine Konfiguration zu nennen. Dieses Dokument beschreibt die Dateistruktur einer gSMC-K und setzt dabei die in [gemSpec\_COS] spezifizierte Funktionalität voraus. Welchem Zweck die hier aufgeführten Dateien, Schlüssel und Passwörter dienen, ist nicht Gegenstand dieses Dokumentes.
    2. Die äußere Gestaltung einer gSMC-K ist in [gemSpec\_SMC\_OPT] festgelegt.

## Methodik

### Nomenklatur

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

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

* In [gemSpec\_COS] wurde ein objektorientierter Ansatz für die Beschreibung der Funktionalität des Betriebssystems gewählt. Deshalb wurde dort der Be­griff "Passwortobjekt" verwendet, wenn Instanzen für eine Benutzerverifikation besprochen wurden. Da in diesem Dokument lediglich numerische Ziffernfolgen als Verifikationsdaten eines Benutzers verwendet werden, wird hier statt Passwortobjekt vielfach der Begriff PIN gewählt, wenn keine Gefahr besteht, dass es zu Verwechslungen kommt zwischen den Verifikationsdaten und der Instanz des Objektes, in denen sie enthalten sind (zur Erinnerung: Ein Passwortobjekt enthält neben den Verifikationsdaten auch einen Identifier, eine Zugriffsregel, eine PUK, …).
  + 1. Bei Referenzierungen wird durch die Zusatzangabe „#Nummer“ auf ein spezifisches Kapitel oder eine Festlegung in dem referenzierten Dokument Bezug genommen.
    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 spezifiziert.
    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 (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:

1. Dabei ist folgendes zu beachten:
2. Für Kommandonachrichten ohne Kommandodaten ist der Term SmCmdEnc sinnlos.
3. Für Antwortnachrichten ohne Antwortdaten ist der Term SmRspEnc sinnlos.
4. 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.
5. 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 der Komponenten zu betrachten. Die normativen Abschnitte tragen deshalb eine Kennzeichnung, aus wessen Sichtweise die Anforderung primär betrachtet wird.

Tabelle 1: Tab\_gSMC-K\_ObjSys\_001 Liste der Komponenten, aus deren Sicht Anforderungen betrachtet werden

|  |  |
| --- | --- |
| Komponente | Beschreibung |
| K\_Initialisierung | Instanz, welche eine Chipkarte im Rahmen der Initialisierung befüllt |
| K\_Personalisierung | Instanz, welche eine Chipkarte im Rahmen der Produktion individualisiert |
| K\_COS | Betriebssystem einer Smartcard |
| K\_externe Welt | Instanz, die außerhalb der Karte liegt |

# 

# Optionen

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

## Option\_Erstellung\_von\_Testkarten

* + 1. **⌦ Card-G2-A\_3250 K\_Personalisierung K\_Initialisierung Vorgaben für die Option\_Erstellung\_von\_Testkarten**
* Die gSMC-K 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. **⌫**

## Option\_Erweiterung\_herstellerspezifische\_Schlüssel\_01

* + 1. Zur sicheren Nutzung des Konnektors benötigen bestimmte Hersteller zusätzliche Schlüsselobjekte auf der gSMC-K, die im MF gespeichert werden sollen.
    2. **⌦ Card-G2-A\_3336 K\_Initialisierung und K\_Personalisierung: Vorgaben für die Option\_Erweiterung\_herstellerspezifische\_Schlüssel\_01**
* Falls eine gSMC-K die Option\_Erweiterung\_herstellerspezifische\_Schlüssel\_01

1. unterstützt, dann MÜSSEN zusätzlich zu allen nicht gekennzeichneten Anforderungen auch alle Anforderungen erfüllt werden, die mit Option\_Erweiterung\_herstellerspezifische\_Schlüssel\_01 gekennzeichnet sind.
2. nicht unterstützt, dann DÜRFEN mit Option\_Erweiterung\_herstellerspezifische\_Schlüssel\_01 gekennzeichnete Anforderungen NICHT relevant für funktionale Tests sein.
3. **⌫**

# 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.

1. Die in diesem Kapitel verwendeten Begriff Vorbereitungsphase und Nutzungsphase werden in [gemSpec\_COS#4] definiert.

# 

# Anwendungsübergreifende Festlegungen

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

## Mindestanzahl logischer Kanäle

* + 1. **⌦ Card-G2-A\_2538 K\_Initialsierung: Anzahl logischer Kanäle**
* Für die Anzahl logischer Kanäle, die von einer gSMC-K 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-K 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\_2873 K\_gSMC-K: Kryptobox**

1. Für das Objektsystem der gSMC-K MUSS ein COS verwendet werden, das die Kryptobox implementiert hat.
2. **⌫**

## Optionale Funktionspakete

### Kontaktlose Schnittstelle

* + 1. **⌦ Card-G2-A\_3040 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\_2995 K\_gSMC-K: USB-Schnittstelle**

Falls eine gSMC-K 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\_2996 K\_gSMC-K: Vorhandensein einer USB-Schnittstelle**

1. Falls eine gSMC-K die Option\_USB\_Schnittstelle nicht nutzen will, KANN für das Objektsystem ein COS verwendet werden,
2. a) das die Option\_USB\_Schnittstelle implementiert hat.
3. b) das die Option\_USB\_Schnittstelle nicht implementiert hat.
4. **⌫**

## Attributstabellen

* + 1. **⌦ Card-G2-A\_2532 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, Passworten und Schlüsseln) in diesem Dokument beziehen sich ausschließlich auf das Security Environment SE#1.
    4. **⌦ Card-G2-A\_2533 K\_Initialisierung: Verwendung von SE#1**
* Alle Objekte MÜSSEN sich in SE#1 wie angegeben verwenden lassen.
  + 1. **⌫**
    2. **⌦ Card-G2-A\_3192 K\_Initialisierung: Verwendbarkeit der Objekte in anderen SEs**

1. Jedes Objekt KANN in SE verwendbar sein, die verschieden sind von SE#1.
2. **⌫**
   * 1. **⌦ Card-G2-A\_3193 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\_2535 K\_Initialisierung: Ordnerattribute**
* Enthält eine Tabelle mit Ordnerattributen

1. keinen applicationIdentifier (AID), so KANN diesem Ordner herstellerspezifisch ein beliebiger AID zugeordnet werden.
2. einen oder mehrere AID, dann MUSS sich dieser Ordner mittels aller angegebenen AID selektieren lassen.
3. keinen fileIdentifier (FID),
4. so DARF dieser Ordner sich NICHT mittels eines *fileIdentifier* aus dem Intervall gemäß [gemSpec\_COS#8.1.1] selektieren lassen, es sei denn es handelt sich um den Ordner *root*, dessen optionaler *fileIdentifier* den Wert ‘3F00’besitzen MUSS.
5. 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\_2536 K\_Initialisierung: Dateiattribute**
* Enthält eine Tabelle mit Attributen einer Datei keinen *shortFileIdentifier*, so DARF sich dieses EF NICHT mittels *shortFileIdentifier* aus dem Intervall gemäß [gemSpec\_COS#8.1.2] selektieren lassen.
  + 1. **⌫**
    2. **⌦ Card-G2-A\_2665 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] gilt:
    2. **⌦ Card-G2-A\_2537 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. **⌫**

## TransportStatus für Passwortobjekte

* + 1. **⌦ Card-G2-A\_3201 K\_Personalisierung und K\_Initialisierung: Zuordnung zu transportStatus für die Passwortobjekte der gSMC-K**
* Die Attribute transportStatus für alle Passwortobjekte dieser Karte (PIN.AK, PIN.NK, PIN.Pers, PIN.SAK, PIN.BNetzA\_RCA, PIN.TSL\_CA) MÜSSEN für eine konkrete Karte denselben Wert aufweisen. Der Wert MUSS aus der Menge {regularPassword, Leer-PIN, Transport-PIN} gewählt werden.
  + 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\_3261 K\_Initialisierung und K\_Personalisierung: Abweichung von Festlegungen zum Zwecke der Personalisierung**
    6. 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.
    7. **⌫**

## Kartenadministration

* + 1. In den Kapiteln 5.3.22 und 5.3.23 sind die Objekte für die zwei verschiedenen Verfahren zur Absicherung der Kommunikation zwischen einem Kartenadministrationssystem (z.B. einem CUpS) und einer Karte beschrieben, die bei der Ausgabe der Karte angelegt werden müssen.
    2. **⌦ Card-G2-A\_2994 K\_Personalisierung: Absicherung der Kartenadministration**

Bei der Personalisierung MUSS der Schlüssel PuK.RCA.ADMIN.CS für die asymmetrische Authentifizierung des Kartenadministrationssystems in die Karte eingebracht werden.

**⌫**

* + 1. **⌦ Card-G2-A\_3592 Symmetrische Kartenadministration**

1. Bei der Personalisierung KÖNNEN die Schlüssel (SK.CMS und SK.CUP) für die symmetrische Authentifizierung des Kartenadministrationssystems in die Karte eingebracht werden.
2. **⌫**
   * 1. **⌦ Card-G2-A\_3593 Schlüsselspeicherung**
3. Der Kartenherausgeber MUSS sicherstellen, dass die Schlüssel zur Absicherung der Kartenadministration mindestens bis zum Ablauf der Zertifikate der Karte sicher verwahrt werden und bei Bedarf an ein Kartenad­ministrationssystem (z.B. ein CUpS) übergeben werden können.
4. **⌫**

# 

# Dateisystem der gSMC-K

* + 1. Dieses Kapitel beschreibt die Konfiguration des Dateisystems, wobei folgende Applikationen berücksichtigt werden:
* MF siehe Kapitel 5.3.1
* DF.AK siehe Kapitel 5.4
* DF.NK siehe Kapitel 5.5
* DF.SAK siehe Kapitel 5.6
* DF.Sicherheitsanker siehe Kapitel 5.7
  + 1. **⌦ Card-G2-A\_2540 K\_Initialisierung: Normative Anforderungen**
* Alle normativen Anforderungen des Kapitels 5 und seiner Unterkapitel MÜSSEN für die gSMC-K gelten.
  + 1. **⌫**
    2. **⌦ Card-G2-A\_2541 K\_Personalisierung: zusätzliche Ordner**
* Die gSMC-K KANN Ordner enthalten, die in diesem Dokument nicht genannt sind.
  + 1. **⌫**
    2. **⌦ Card-G2-A\_2542 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 gemäß [gemSpec\_COS] enthält folgende Attribute:
    2. **⌦ Card-G2-A\_2543 K\_Initialisierung: Wert des Attributes *root***
* Der Wert des Attributes *root* MUSS die Anwendung gemäß Tab\_gSMC-K\_ObjSys\_004 sein.
  + 1. **⌫**
    2. **⌦ Card-G2-A\_2544 K\_Personalisierung und K\_Initialisierung: Wert des Attributes answerToReset**
* Die Werte der Attribute coldAnswerToReset und warmAnswerToReset MÜSSEN den Vorgaben der Anforderungen Card-G2-A\_2547, Card-G2-A\_2548, Card-G2-A\_2997 und Card-G2-A\_3041 entsprechen.
  + 1. **⌫**
    2. **⌦ Card-G2-A\_2545 K\_Personalisierung: Wert des Attributes iccsn8**
* Der Wert des Attributes *iccsn8* MUSS identisch zu den letzten acht Oktetten im *body* von EF.GDO sein (siehe Kapitel 5.3.5).
  + 1. **⌫**
    2. **⌦ Card-G2-A\_2546 K\_Initialisierung: Inhalt persistentPublicKeyList**
* In der *persistentPublicKeyList* MÜSSEN alle in dieser Spezifikation enthaltenen öffentlichen Schlüssel enthalten sein.
  + 1. **⌫**
    2. **⌦ Card-G2-A\_3191 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\_3268 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\_3514 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 ATR-Kodierung

* + 1. Für die gSMC-K gelten die Konventionen für die technischen Eigenschaften, ATR und Über­tragungsprotokolle aus [gemSpec\_COS] für die elektrische Schnittstelle. Die gSMC-K ist als Plug-In-Karte (ID-000) für die Nutzung in entsprechenden Kartenterminals vorgesehen.
    2. **⌦ Card-G2-A\_2547 K\_Personalisierung und K\_Initialisierung: ATR-Kodierung**
* Die ATR-Kodierung MUSS die in Tab\_gSMC-K\_ObjSys\_002 dargestellten Werte besitzen.

Tabelle 2: Tab\_gSMC-K\_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 (maximal 15 Oktett) |
| TCK | XOR | Check Character (exclusive OR) |

* + 1. **⌫**
    2. **⌦ Card-G2-A\_2548 K\_Personalisierung und K\_Initialisierung: TC1 Byte im 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\_2997 K\_Personalisierung und K\_Initialisierung: Historical Bytes im ATR**

1. Das Attribut answerToReset SOLL keine Historical Bytes enthalten.
2. **⌫**
   * 1. **⌦ Card-G2-A\_3041 K\_Personalisierung und K\_Initialisierung: Vorgaben für Historical Bytes**
3. 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

* In dem zugehörenden Kapitel sind alle Objekte eines Typs gemeinsam dargestellt; die jeweils gültigen Parameter sind in einer Tabelle beschrieben.
  + 1. Die Abbildung 1 zeigt die allgemeine Struktur der gSMC-K.
    2. 

Abbildung 1: Abb\_gSMC-K\_ObjSys\_001 Dateistruktur einer gSMC-K auf oberster Ebene

## Root-Anwendung und Dateien auf MF-Ebene

### MF

* + 1. Diese Applikation beinhaltet allgemeine Datenelemente und Informationen, die dem Betrieb der Chipkarte als solche dienen, oder allen Anwendungen gleichermaßen zur Verfügung stehen.
    2. **⌦ Card-G2-A\_2553 K\_Initialisierung: Initialisierte Attribute von MF**
* MF MUSS die in Tab\_gSMC-K\_ObjSys\_004 dargestellten Werte besitzen.

Tabelle 3: Tab\_gSMC-K\_ObjSys\_004 - Initialisierte Attribute von MF

| Attribute | Wert | Bemerkung |
| --- | --- | --- |
| Objekttyp | Ordner |  |
| *applicationIdentifier* | ‘D276 0001 4480 01’ |  |
| *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 | PWD(PIN.Pers)  OR AUT\_CMS |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (3) |
| Zugriffsregel für logischen LCS „Termination state“ | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (3) |

* + 1. **⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem Ordnerobjekt arbeiten, sind:   
   Activate, Deactivate, Delete, Fingerprint, Get Random, 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 5.3 im Allgemeinen irrelevant.

### MF / EF.ATR

* + 1. Die transparente Datei EF.ATR enthält Informationen zur maximalen Größe einer APDU in Sende- und Empfangsrichtung sowie zur Identifizierung des Betriebssystems.
    2. **⌦ Card-G2-A\_2554 K\_Initialisierung: Initialisierte Attribute von MF / EF.ATR**
* Das Objekt EF.ATR MUSS die in Tab\_gSMC-K\_ObjSys\_005 dargestellten Werte besitzen.

Tabelle 4: Tab\_gSMC-K\_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] |  |
| 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 (3) |
| Zugriffsregel für logischen LCS „Termination state“ | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (3) |

* + 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 [ISO7816-4] festgelegt.
   * 1. **⌦ Card-G2-A\_3251 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 Anwendungs-Templates gemäß [ISO7816-4].
    2. **⌦ Card-G2-A\_2563 K\_Initialisierung: Initialisierte Attribute von MF / EF.DIR**
* Das Objekt EF.DIR MUSS die in Tab\_gSMC-K\_ObjSys\_009 dargestellten Werte besitzen.

Tabelle 5: Tab\_gSMC-K\_ObjSys\_009 Initialisierte Attribute von MF / EF.DIR

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute | Wert | Bemerkung | |
| Objekttyp | linear variables Elementary File |  | |
| *fileIdentifier* | ‘2F 00’ | siehe Hinweis (7) | |
| *shortFileIdentifier* | ‘1E’ = 30 | siehe Hinweis (7) | |
| *numberOfOctet* | ‘006E’ Oktett = 110 Oktett |  | |
| *maxNumRecords* | 8 Rekord |  | |
| *maxRecordLength* | 32 Oktett |  | |
| *flagRecordLCS* | False |  | |
| *flagTransactionMode* | True |  | |
| *flagChecksum* | True |  | |
| *lifeCycleStatus* | „Operational state (activated)“ |  | |
| *shareable* | True |  | |
| *recordList*  Rekord 1  Rekord 2  Rekord 3  Rekord 4  Rekord 5    Rekord 6  … | ‘61-09-(4F 07 D27600014480 01)’  ‘61-08-(4F 06’D27600014402)’  ‘61-08-(4F 06 D27600014403)’  ‘61-08-(4F 06 D27600014404)’  ‘61-08-(4F 06 D27600014405)’  nicht vorhanden, MUSS mittels Append Record angelegt werden  … | MF siehe 5.3.1  AK siehe 5.4  NK siehe 5.5  SAK, siehe 5.6  Sicherheitsanker siehe 5.7  siehe Hinweis (8) | |
| Zugriffsregel für logischen LCS „Operational state (activated)” | | | |
| Zugriffsart | Zugriffsbedingung | | Bemerkung |
| Append Record | PWD(PIN.Pers)  OR AUT\_CMS | | siehe Hinweis (9) |
| Delete Record | 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 (3) |
| Zugriffsregel für logischen LCS „Termination state“ | | | |
| Zugriffsart | Zugriffsbedingung | | Bemerkung |
| alle | herstellerspezifisch | | siehe Hinweis (3) |

* + 1. **⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem linear variablen EF arbeiten, sind:   
   Activate, Activate Record, Append Record, Deactivate, DeactivateRecord, Delete, Delete Record, Erase Record, Read Record, Search Record, Select, Terminate, Update Record, Write Record.
2. Die Werte von fileIdentifier und shortFileIdentifier sind in [ISO7816-4] festgelegt.
3. Weitere Records existieren nur, wenn optionale Applikationen vorhanden sind.
4. Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 5.10.

### MF / EF.EnvironmentSettings

* + 1. In EF.EnvironmentSettings wird die Information gespeichert, über welche der Konnektor erkennen kann, in welcher Umgebung er betrieben wird.
    2. **⌦ Card-G2-A\_2565 K\_Initialisierung: Initialisierte Attribute von MF / EF.EnvironmentSettings**
* Das Objekt EF.EnvironmentSettings MUSS die in Tab\_gSMC-K\_ObjSys\_010 dargestellten Werte besitzen.

Tabelle 6: Tab\_gSMC-K\_ObjSys\_010 Initialisierte Attribute von MF / EF.EnvironmentSettings

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ‘2F 13’ |  |
| *shortFileIdentifier* | ‘13’ = 19 |  |
| *numberOfOctet* | ’0100’ Oktett = 256 Oktett |  |
| *positionLogicalEndOfFile* | ’0’ | wird personalisiert |
| *flagTransactionMode* | False |  |
| *flagChecksum* | True |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *shareable* | True |  |
| *body* | kein Inhalt | 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 (3) |
| Zugriffsregel für logischen LCS „Termination state“ | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (3) |

* + 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. **⌦ Card-G2-A\_3394 K\_Personalisierung: Personalisierte Attribute von MF / EF.EnvironmentSettings**

* Bei der Personalisierung von EF.EnvironmentSettings MÜSSEN die in Tab\_gSMC-K\_ObjSys\_090 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 7: Tab\_gSMC-K\_ObjSys\_090 Attribute von MF / EF.EnvironmentSettings

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| *positionLogicalEndOfFile* | 1 |  |
| *body* | gemäß [gemSpec\_Karten\_Fach\_TIP] |  |

* + 1. **⌫**

### MF / EF.GDO

* + 1. In EF.GDO wird das Datenobjekt ICCSN gespeichert, welches die Kennnummer der Karte enthält.
    2. **⌦ Card-G2-A\_2566 K\_Initialisierung: Initialisierte Attribute von MF / EF.GDO**
* Das Objekt EF.GDO MUSS die in Tab\_gSMC-K\_ObjSys\_011 dargestellten Werte besitzen.



Tabelle 8: Tab\_gSMC-K\_ObjSys\_011 Initialisierte Attribute von MF / EF.GDO

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ‘2F 02’ |  |
| *shortFileIdentifier* | ‘02’ = 2 |  |
| *numberOfOctet* | ‘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 (3) |
| Zugriffsregel für logischen LCS „Termination state“ | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (3) |

* + 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. **⌦ Card-G2-A\_2567 K\_Personalisierung: Personalisiertes Attribut von EF.GDO**

* Bei der Personalisierung von EF.GDO MÜSSEN die in Tab\_gSMC-K\_ObjSys\_177 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 9: Tab\_gSMC-K\_ObjSys\_177 Personalisierte Attribute von MF / EF.GDO

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| *positionLogicalEndOfFile* | ‘0C’ 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\_3392 K\_Initialisierung: Attribute von MF / EF.KeyInfo**
* EF.KeyInfo MUSS die in Tab\_gSMC-K\_ObjSys\_150 dargestellten initialisierten Attribute besitzen.

Tabelle 10: Tab\_ gSMC-K\_ObjSys\_150 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 (13) |
| 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- / CUP-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.
    3. **⌦ Card-G2-A\_2568 K\_Initialisierung: Initialisierte Attribute von MF / EF.Version2**
* Das Objekt EF.Version2 MUSS die in Tab\_gSMC-K\_ObjSys\_012 dargestellten Werte besitzen.



Tabelle 11 Tab\_gSMC-K\_ObjSys\_012 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 (15) |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (3) |
| Zugriffsregel für logischen LCS „Termination state“ | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (3) |

* + 1. **⌫**

1. Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kap.5.10.

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

* + 1. Diese Datei enthält ein CV–Zertifikat für die Kryptographie mit elliptischen Kurven gemäß [gemSpec\_COS], welches den öffentlichen Schlüssel PuK.CA\_SAK.CS.E256 einer CA enthält. Das Zertifikat lässt sich mittels MF / PuK.RCA.CS.E256 (siehe Kapitel 5.3.21) prüfen. Der im Zertifikat enthaltene öffentliche Schlüssel dient der Verifizierung von weiteren Zertifikaten, die im Dateisystem enthalten sind (siehe zum Beispiel Kapitel 5.6.8).
    2. **⌦ Card-G2-A\_2561 K\_Initialisierung: Initialisierte Attribute von MF / EF.C.CA\_SAK.CS.E256**
* Das Objekt EF.C.CA\_SAK.CS.E256 MUSS die in Tab\_gSMC-K\_ObjSys\_007 darge­stellten Werte besitzen.

Tabelle 12: Tab\_gSMC-K\_ObjSys\_007 Initialisierte Attribute von MF / EF.C.CA\_SAK.CS.E256

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute | Wert | Bemerkung | |
| *Objekttyp* | transparentes Elementary File |  | |
| *fileIdentifier* | ‘2F 07’ |  | |
| *shortFileIdentifier* | ‘07’ = 7 |  | |
| *numberOfOctet* | ‘011D’ Oktett = 285 Oktett |  | |
| *positionLogicalEndOfFile* | Wildcard | 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 (17) |
| Read Binary | ALWAYS |  |
| Set Logical EOF  Write Binary | AUT\_CMS OR AUT\_CUP | siehe Hinweis (17) |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (3) |
| Zugriffsregel für logischen LCS „Termination state“ | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (3) |

* + 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 5.10.
   * 1. **⌦ Card-G2-A\_3393 K\_Personalisierung: Personalisierte Attribute von MF / EF.C.CA\_SAK.CS.E256**

* Bei der Personalisierung von EF.C.CA\_SAK.CS.E256 MÜSSEN die in Tab\_gSMC-K\_ObjSys\_087 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 13: Tab\_gSMC-K\_ObjSys\_087 Attribute von MF / EF.C.CA\_SAK.CS.E256

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| *positionLogicalEndOfFil*e | ‘00DC’ Oktett = 220 Oktett |  |
| *body* | C.CA\_SAK.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\_SAK.CS.E384

* + 1. Diese Datei enthält ein CV-Zertifikat für die Kryptographie mit elliptischen Kurven gemäß [gemSpec\_COS], welches den öffentlichen Schlüssel PuK.CA\_SAK.CS.E384 einer CA enthält. Der im Zertifikat enthaltene öffentliche Schlüssel dient der Verifizierung von weiteren Zertifikaten, die im Dateisystem enthalten sind (siehe zum Beispiel Kapitel 5.6.10).
    2. **⌦ Card-G2-A\_2562 K\_Initialisierung: Initialisierte Attribute von MF / EF.C.CA\_SAK.CS.E384**
* Das Objekt EF.C.CA\_SAK.CS.E384 MUSS die in Tab\_gSMC-K\_ObjSys\_008 dargestellten Werte besitzen.

Tabelle 14: Tab\_gSMC-K\_ObjSys\_008 Initialisierte Attribute von MF / EF.C.CA\_SAK.CS.E384

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ‘2F 0D’ |  |
| *shortFileIdentifier* | ‘0D’ = 13 |  |
| *numberOfOctet* | ‘011D’ Oktett = 285 Oktett |  |
| *positionLogicalEndOfFile* | ’0’ |  |
| *flagTransactionMode* | True |  |
| *flagChecksum* | False |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *shareable* | True |  |
| *body* | kein Inhalt | wird später nachgeladen |
| Zugriffsregeln | | |
| *accessRules* | identisch zu EF.C.CA\_SAK.CS.E256 |  |

* + 1. **⌫**

### MF / EF.PuK.RCA.CS.R2048

* + 1. Diese Datei enthält den öffentlichen Schlüssel der CVC-Root-CA der Generation 1 . Das Zertifikat kann vom Konnektor ausgelesen werden, um mit dem Schlüssel als Gegenstelle einer eGK G1 deren Echtheit zu überprüfen.
    2. **⌦ Card-G2-A\_3252 K\_Initialisierung: Initialisierte Attribute von MF / EF.PuK.RCA.CS.R2048**
* Das Objekt EF.PuK.RCA.CS.R2048 MUSS die in Tab\_gSMC-K\_ObjSys\_176 dargestellten Werte besitzen.

Tabelle 15: Tab\_gSMC-K\_ObjSys\_176 Initialisierte Attribute von MF / EF.PuK.RCA.CS.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ‘2F 14’ |  |
| *shortFileIdentifier* | ‘14’ = 20 |  |
| *numberOfOctet* | ‘01 10’ Oktett = 272 Oktett |  |
| *positionLogicalEndOfFile* | Zahl der tatsächlich belegten Oktette |  |
| *flagTransactionMode* | False |  |
| *flagChecksum* | True |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *shareable* | True |  |
| Für Echtkarten MUSS das nachfolgende Attribut mit dem unten angegebenen Wert initialisiert werden.  Für Option\_Erstellung\_von\_Testkarten MUSS das nachfolgende Attribut mit Wildcard oder AttributeNotSet initialisiert werden. | | |
| *body* | Öffentlicher Schlüssel mit Moduluslänge  2048 Bit, TLV-codiert mit dem Wert der CVC-Root-CA aus der PU gemäß [gemSpec\_CVC\_TSP#4.5] |  |
| Zugriffsregel für logischen LCS „Operational state (activated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Read Binary | ALWAYS |  |
| Delete | AUT\_CMS OR AUT\_CUP | siehe Hinweis (21) |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (3) |
| Zugriffsregel für logischen LCS „Termination state“ | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (3) |

* + 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 5.10.
   * 1. **⌦ Card-G2-A\_3580 K\_Personalisierung: Personalisierte Attribute von MF / EF.PuK.RCA.CS.R2048 für Testkarten**

* Bei der Personalisierung von EF.PuK.RCA.CS.R2048 für Testkarten MUSS das in Tab\_gSMC-K\_ObjSys\_148 angegebene Attribut mit dem dort angegebenen Inhalt personalisiert werden.

Tabelle 16:Tab\_gSMC-K\_ObjSys\_148 Personalisierte Attribute von MF / EF.PuK.RCA.CS.R2048 für Testkarten

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| *body* | Öffentlicher Schlüssel mit Moduluslänge 2048 Bit, TLV-codiert,  mit dem Wert der CVC-Root-CA aus der RU/TU | Details siehe [gemSpec\_TK#3.1.2] |

* + 1. **⌫**

### MF / EF.C.RCA.CS.E256

Diese Datei enthält den zum Zeitpunkt der gSMC-K-Produktion ältesten noch verwendbaren Schlüssel PuK.RCA.CS.E256 in Form eines „self-signed“ CV-Zertifikates. Das Zertifikat kann vom Konnektor ausgelesen werden, um mit dem Schlüssel als Gegenstelle einer eGK G2 deren Echtheit zu überprüfen.

* + 1. **⌦ Card-G2-A\_2666 K\_Initialisierung: Initialisierte Attribute von MF / EF.C.RCA.CS.E256**
* Das Objekt EF.C.RCA.CS.E256 MUSS die in Tab\_gSMC-K\_ObjSys\_084 dargestellten Werte besitzen.

Tabelle 17: Tab\_gSMC-K\_ObjSys\_084 Initialisierte Attribute von MF / EF.C.RCA.CS.E256

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ‘2F 15’ |  |
| *shortFileIdentifier* | ‘15’ = 21 |  |
| *numberOfOctet* | ‘DC’ Oktett = 220 Oktett |  |
| *positionLogicalEndOfFile* | Zahl der tatsächlich belegten Oktette |  |
| *flagTransactionMode* | True |  |
| *flagChecksum* | True |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *shareable* | True |  |
| Für Echtkarten MUSS das nachfolgende Attribut mit dem unten angegebenen Wert initialisiert werden.  Für Option\_Erstellung\_von\_Testkarten MUSS das nachfolgende Attribut mit Wildcard oder AttributeNotSet initialisiert werden. | | |
| *body* | „self-signed“ CV-Zertifikat mit einem öffentlichen  Schlüssel mit Domainparameter = brainpoolP256r1 codiert gemäß [TR-03110-3#Table 17] mit dem Wert der CVC-Root-CA aus der PU gemäß [gemSpec\_CVC\_TSP#4.5] |  |
| Zugriffsregel für logischen LCS „Operational state (activated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Read Binary | ALWAYS |  |
| Delete | AUT\_CMS OR AUT\_CUP | siehe Hinweis (21) |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (3) |
| Zugriffsregel für logischen LCS „Termination state“ | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (3) |

* + 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 5.10.
   * 1. **⌦ Card-G2-A\_3581 K\_Personalisierung: Personalisierte Attribute von MF /**  **EF.C.RCA.CS.E256** **für Testkarten**

* Bei der Personalisierung von EF.C.RCA.CS.E256 für Testkarten MUSS das in Tab\_gSMC-K\_ObjSys\_149 angegebene Attribut mit dem dort angegebenen Inhalt personalisiert werden.

Tabelle 18:Tab\_gSMC-K\_ObjSys\_149 Personalisierte Attribute von MF / EF.C.RCA.CS.E256 für Testkarten

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| *body* | „self-signed“ CV-Zertifikat mit einem öffentlichen  Schlüssel mit Domainparameter = brainpoolP256r1 codiert gemäß [TR-03110-3#Table 17] mit dem Wert der CVC-Root-CA aus der RU/TU | gemäß [gemSpec\_TK#3.1.2] |

* + 1. **⌫**

### MF / EF.C.SMC.AUT\_CVC.E256

* + 1. Diese Datei enthält ein CV-Zertifikat für die Kryptographie mit elliptischen Kurven gemäß [gemSpec\_PKI], welches den öffentlichen Schlüssel PuK.SMC.AUT\_CVC.E256 zum zugehörigen privaten Schlüssel (siehe Kapitel 5.3.18) enthält. Dieses Zertifikat lässt sich mittels des öffentlichen Schlüssels aus EF.C.CA\_SAK.CS.E256 (siehe Kapitel 5.3.8) prüfen.
    2. **⌦ Card-G2-A\_3280 K\_Initialisierung: Initialisierte Attribute von MF /** EF.C.SMC.AUT\_CVC.E256
* EF.C.SMC.AUT\_CVC.E256 MUSS die in Tab\_gSMC-K\_ObjSys\_192 dargestellten Attribute besitzen.

Tabelle 19: Tab\_gSMC-K\_ObjSys\_192 Initialisierte Attribute von MF / EF.C.SMC.AUT\_CVC.E256

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ‘2F 0A’ |  |
| *shortFileIdentifier* | ‘0A’ = 10 |  |
| *numberOfOctet* | ’01 1F’ Oktett = 287 Oktett |  |
| *positionLogicalEndOfFile* | Wildcard | wird personalisiert |
| *flagTransactionMode* | True |  |
| *flagChecksum* | False |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *shareable* | True |  |
| *body* | Wildcard | wird personalisiert |
| Zugriffsregel für logischen LCS „Operational state (activated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Delete | AUT\_CMS OR AUT\_CUP |  |
| Read Binary | ALWAYS |  |
| Set Logical EOF  Write Binary | AUT\_CMS OR AUT\_CUP |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state“ | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |

* + 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 eine Flagliste mit dem Wert ’00…00’.
   * 1. **⌦ Card-G2-A\_3328 K\_Personalisierung: Festlegung von CHR für** EF.C.SMC.AUT\_CVC.E256

* Falls das asymmetrische Authentifizierungsverfahren genutzt werden soll, dann MUSS bei der Personalisierung für die CHR des Zertifikates CHR = ‘00 05’ || ICCSN gelten, wobei die ICCSN denselben Wert besitzen MUSS, wie das Wertfeld *body* aus [Card-G2-A\_2567].
  + 1. **⌫**
    2. **⌦ Card-G2-A\_3329 K\_Personalisierung: Personalisierte Attribute von MF /** EF.C.SMC.AUT\_CVC.E256
* Falls das asymmetrische Authentifizierungsverfahren genutzt werden soll, dann MÜSSEN bei der Personalisierung von EF.C.SMC.AUT\_CVC.E256 die in Tab\_gSMC-K\_ObjSys\_193 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.
  + 1. **Tabelle 20: Tab\_gSMC-K\_ObjSys\_193 Personalisierte Attribute von MF / EF.C.SMC.AUT\_CVC.E256**

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| *positionLogicalEndOfFile* | ‘00 DE’ Oktett = 222 Oktett |  |
| *body* | C.SMC.AUT\_CVC.E256 gemäß [gemSpec\_PKI] |  |

* + 1. **⌫**

### MF / EF.C.SMC.AUT\_CVC.E384

* + 1. Diese Datei enthält ein CV-Zertifikat für die Kryptographie mit elliptischen Kurven gemäß [gemSpec\_PKI], welches den öffentlichen Schlüssel PuK.SMC.AUT\_CVC.E384 zum zugehörigen privaten Schlüssel (siehe Kapitel 5.3.19) enthält. Dieses Zertifikat lässt sich mittels des öffentlichen Schlüssels aus EF.C.CA\_SAK.CS.E384 (siehe Kapitel 5.3.9) prüfen.
    2. **⌦ Card-G2-A\_3330 K\_Initialisierung: Initialisierte Attribute von MF / EF.C.SMC.AUT\_CVC.E384**
    3. EF.C.SMC.AUT\_CVC.E384 MUSS die in Tab\_gSMC-K\_ObjSys\_194 dargestellten Attribute besitzen.
    4. **Tabelle 21: Tab\_gSMC-K\_ObjSys\_194 Initialisierte Attribute von MF / EF.C.SMC.AUT\_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* | kein Inhalt |  |
| Zugriffsregel | | |
| *accessRules* | identisch zu EF.C.SMC.AUT\_CVC.E256 |  |

* + 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 eine Flagliste mit dem Wert ’00…00’.
   * 1. **⌦ Card-G2-A\_3331 K\_externe Welt: Festlegung von CHR für EF.C.SMC.AUT\_CVC.E384**
     2. Falls das asymmetrische Authentifizierungsverfahren genutzt wird, dann MUSS bei der Erstellung des Zertifikats C.SMC.AUT\_CVC.E384 für die CHR gelten: CHR = ‘00 06’ || ICCSN , wobei die ICCSN denselben Wert besitzen MUSS, wie das Wertfeld *body* aus [Card-G2-A\_2567].
     3. **⌫**

### MF / PIN.AK

* + 1. Dieses Passwortobjekt wird zur Freischaltung von gewissen Operationen im DF.AK (siehe Kapitel 5.4) verwendet.
    2. **⌦ Card-G2-A\_2569 K\_Initialisierung: Initialisierte Attribute von MF / PIN.AK**
* Das Objekt PIN.AK MUSS die in Tab\_gSMC-K\_ObjSys\_013 dargestellten Werte besitzen.

Tabelle 22: Tab\_gSMC-K\_ObjSys\_013 Initialisierte Attribute von MF / PIN.AK

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | Passwortobjekt |  |
| *pwdIdentifier* | ‘00’ = 0 |  |
| *secret* | undefiniert | wird personalisiert |
| *minimumLength* | 12 |  |
| *maximumLength* | 12 |  |
| *startRetryCounter* | 3 |  |
| *retryCounter* | 3 |  |
| *transportStatus* | ein Wert aus der Menge {Leer–PIN, Transport–PIN} |  |
| *flagEnabled* | True |  |
| *startSsec* | unendlich |  |
| *PUK* | kein Inhalt | keine PUK |
| *pukUsage* | 0 | keine PUK |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregel für logischen LCS „Operational state (activated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Change RD, P1=1 | ALWAYS | siehe Hinweis (27) |
| herstellerspezifisch | siehe Hinweis (27) |
| Change RD, P1=0 | ALWAYS | siehe Hinweis (28) |
| Disable Verification Requirement | PWD(PIN.AK) |  |
| Enable  Verification Requirement | ALWAYS |  |
| Get Pin Status | ALWAYS |  |
| Verify | ALWAYS |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (3) |
| Zugriffsregel für logischen LCS „Termination state“ | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (3) |

* + 1. **⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem Passwortobjekt arbeiten, sind: Activate, Change Reference Data, Deactivate, Delete, Disable Verification Requirement, Enable Verification Requirement, Get Pin Status, Reset Retry Counter, Verify, Terminate.
2. Diese Tabellenzeile gilt für den Fall transportStatus gleich Leer-PIN.
3. Diese Tabellenzeile gilt für den Fall transportStatus ungleich Leer-PIN.
   * 1. **⌦ Card-G2-A\_2570 K\_Initialisierung: CHANGE REFERENCE DATA bei Nutzung der Leer-PIN für PIN.AK**

* Wenn für PIN.AK als Transportschutz Leer-PIN verwendet wird, dann DARF PIN.AK nicht personalisiert werden und es DARF im Zustand *transportStatus* gleich *regularPassword* das Attribut *secret* NICHT mit der Variante Change Reference Data mit P1=1 änderbar sein. Die letzte Anforderung ist herstellerspezifisch umzusetzen.
  + 1. **⌫**
    2. **⌦ Card-G2-A\_3396 K\_Personalisierung: Personalisierte Attribute von MF / PIN.AK**
* Wenn der Wert des Attributes transportStatus Transport–PIN ist, MÜSSEN bei der Personalisierung von PIN.AK die in Tab\_gSMC-K\_ObjSys\_094 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 23: Tab\_gSMC-K\_ObjSys\_094 Attribute von MF / PIN.AK

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| *secret* | PIN-Wert gemäß [gemSpec\_PINPUK\_TI] | wird personalisiert |
| *transportStatus* | Transport-PIN | wird gegebenenfalls personalisiert, siehe Hinweis (29) |

* + 1. **⌫**

1. Für transportStatus wird der Wert „Transport-PIN“ initialisiert. Beispielsweise durch das Kommando Change Reference Data ist es möglich, diesen Wert im Rahmen der Personalisierung auf „regularPassword“ zu setzen.

### MF / PIN.NK

* + 1. Dieses Passwortobjekt wird zur Freischaltung von gewissen Operationen im DF.NK (siehe Kapitel 5.5) verwendet.
    2. **⌦ Card-G2-A\_2571 K\_Initialisierung: Initialisierte Attribute von MF / PIN.NK**
* Das Objekt PIN.NK MUSS die in Tab\_gSMC-K\_ObjSys\_014 dargestellten Werte besitzen.

Tabelle 24: Tab\_gSMC-K\_ObjSys\_014 Initialisierte Attribute von MF / PIN.NK

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | Passwortobjekt |  |
| *pwdIdentifier* | ‘01’ = 1 |  |
| *secret* | undefiniert | wird personalisiert |
| *minimumLength* | 12 |  |
| *maximumLength* | 12 |  |
| *startRetryCounter* | 3 |  |
| *retryCounter* | 3 |  |
| *transportStatus* | ein Wert aus der Menge {Leer–PIN, Transport–PIN} |  |
| *flagEnabled* | True |  |
| *startSsec* | unendlich |  |
| *PUK* | kein Inhalt | keine PUK |
| *pukUsage* | 0 | keine PUK |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregel für logischen LCS „Operational state (activated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Change RD, P1=1 | ALWAYS | siehe Hinweis (31) |
| herstellerspezifisch | siehe [Card-G2-A\_2572] |
| Change RD, P1=0 | ALWAYS | siehe Hinweis (32) |
| Disable Verification Requirement | PWD(PIN.NK) |  |
| Enable  Verification Requirement | ALWAYS |  |
| Get Pin Status | ALWAYS |  |
| Verify | ALWAYS |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (3) |
| Zugriffsregel für logischen LCS „Termination state“ | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (3) |

* + 1. **⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem Passwortobjekt arbeiten, sind: Activate, Change Reference Data, Deactivate, Delete, Disable Verification Requirement, Enable Verification Requirement, Get Pin Status, Reset Retry Counter, Verify, Terminate.
2. Diese Tabellenzeile gilt für den Fall transportStatus gleich Leer-PIN.
3. Diese Tabellenzeile gilt für den Fall transportStatus ungleich Leer-PIN.
   * 1. **⌦ Card-G2-A\_2572 K\_Initialisierung: CHANGE REFERENCE DATA bei Nutzung der Leer-PIN für PIN.NK**

* Wenn für PIN.NK als Transportschutz Leer-PIN verwendet wird, dann DARF PIN.NK nicht personalisiert werden und es DARF im Zustand *transportStatus* gleich *regularPassword* das Attribut *secret* NICHT mit der Variante Change Reference Data mit P1=1 änderbar sein. Die letzte Anforderung ist herstellerspezifisch umzusetzen.
  + 1. **⌫**
    2. **⌦ Card-G2-A\_3397 K\_Personalisierung: Personalisierte Attribute von MF / PIN.NK**
* Wenn der Wert des Attributes transportStatus Transport–PIN ist, MÜSSEN bei der Personalisierung von PIN.NK die in Tab\_gSMC-K\_ObjSys\_095 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 25: Tab\_gSMC-K\_ObjSys\_095 Attribute von MF / PIN.NK

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| *secret* | PIN-Wert gemäß [gemSpec\_PINPUK\_TI] | wird personalisiert |
| *transportStatus* | Transport-PIN | wird gegebenenfalls personalisiert,  siehe Hinweis (33) |

* + 1. **⌫**

1. Für transportStatus wird der Wert „Transport-PIN“ initialisiert. Beispielsweise durch das Kommando Change Reference Data ist es möglich, diesen Wert im Rahmen der Personalisierung auf „regularPassword“ zu setzen.

### MF / PIN.Pers

* + 1. Dieses Passwortobjekt wird zur Freischaltung verwendet, wenn im *root*-Verzeichnis neue Dateien oder Applikationen anzulegen sind.
    2. **⌦ Card-G2-A\_2573 K\_Initialisierung: Initialisierte Attribute von MF / PIN.Pers**
* Das Objekt PIN.Pers MUSS die in Tab\_gSMC-K\_ObjSys\_015 dargestellten Werte besitzen.

Tabelle 26: Tab\_gSMC-K\_ObjSys\_015 Initialisierte Attribute von MF / PIN.Pers

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | Passwortobjekt |  |
| *pwdIdentifier* | ‘02’ = 2 |  |
| *secret* | undefiniert | wird personalisiert |
| *minimumLength* | 12 |  |
| *maximumLength* | 12 |  |
| *startRetryCounter* | 3 |  |
| *retryCounter* | 3 |  |
| *transportStatus* | ein Wert aus der Menge {Leer–PIN, Transport–PIN} |  |
| *flagEnabled* | True |  |
| *startSsec* | unendlich |  |
| *PUK* | kein Inhalt | keine PUK |
| *pukUsage* | 0 | keine PUK |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregel für logischen LCS „Operational state (activated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Change RD, P1=1 | ALWAYS | siehe Hinweis (35) |
| herstellerspezifisch | siehe [Card-G2-A\_2574] |
| Change RD, P1=0 | ALWAYS | siehe Hinweis (36) |
| Disable Verification Requirement | PWD(PIN.Pers) |  |
| Enable  Verification Requirement | ALWAYS |  |
| Get Pin Status | ALWAYS |  |
| Verify | ALWAYS |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (3) |
| Zugriffsregel für logischen LCS „Termination state“ | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (3) |

* + 1. **⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem Passwortobjekt arbeiten, sind: Activate, Change Reference Data, Deactivate, Delete, Disable Verification Requirement, Enable Verification Requirement, Get Pin Status, Reset Retry Counter, Verify, Terminate.
2. Diese Tabellenzeile gilt für den Fall transportStatus gleich Leer-PIN.
3. Diese Tabellenzeile gilt für den Fall transportStatus ungleich Leer-PIN.
   * 1. **⌦** **Card-G2-A\_2574 K\_Initialisierung: CHANGE REFERENCE DATA bei Nutzung der Leer-PIN für PIN.Pers**

* Wenn für PIN.Pers als Transportschutz Leer-PIN verwendet wird, dann DARF PIN.Pers nicht personalisiert werden und es DARF im Zustand *transportStatus* gleich *regularPassword* das Attribut *secret* NICHT mit der Variante Change Reference Data mit P1=1 änderbar sein. Die letzte Anforderung ist herstellerspezifisch umzusetzen.
  + 1. **⌫**
    2. **⌦ Card-G2-A\_3398 K\_Personalisierung: Personalisierte Attribute von MF / PIN.Pers**
* Wenn der Wert des Attributes transportStatus Transport–PIN ist, MÜSSEN bei der Personalisierung von PIN.Pers die in Tab\_gSMC-K\_ObjSys\_096 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 27: Tab\_gSMC-K\_ObjSys\_096 Attribute von MF / PIN.Pers

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| *secret* | PIN-Wert gemäß [gemSpec\_PINPUK\_TI] | wird personalisiert |
| *transportStatus* | Transport-PIN | Wird gegebenenfalls personalisiert, Hinweis (37) |

* + 1. **⌫**

1. Für transportStatus wird der Wert „Transport-PIN“ initialisiert. Beispielsweise durch das Kommando Change Reference Data ist es möglich, diesen Wert im Rahmen der Personalisierung auf „regularPassword“ zu setzen.

### MF / PIN.SAK

* + 1. Dieses Passwortobjekt wird zur Freischaltung von gewissen Operationen im DF.SAK (siehe Kapitel **5.6**) verwendet.
    2. **⌦ Card-G2-A\_2575 K\_Initialisierung: Initialisierte Attribute von MF / PIN.SAK**
* Das Objekt PIN.SAK MUSS die in Tab\_gSMC-K\_ObjSys\_016 dargestellten Werte besitzen.

Tabelle 28: Tab\_gSMC-K\_ObjSys\_016 Initialisierte Attribute von MF / PIN.SAK

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | Passwortobjekt |  |
| *pwdIdentifier* | ‘03’ = 3 |  |
| *secret* | undefiniert | wird personalisiert |
| *minimumLength* | 12 |  |
| *maximumLength* | 12 |  |
| *startRetryCounter* | 3 |  |
| *retryCounter* | 3 |  |
| *transportStatus* | ein Wert aus der Menge {Leer–PIN, Transport–PIN} |  |
| *flagEnabled* | True |  |
| *startSsec* | unendlich |  |
| *PUK* | kein Inhalt | keine PUK |
| *pukUsage* | 0 | keine PUK |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregel für logischen LCS „Operational state (activated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Change RD, P1=1 | ALWAYS | siehe Hinweis (39) |
| herstellerspezifisch | siehe [Card-G2-A\_2576] |
| Change RD, P1=0 | ALWAYS | siehe Hinweis (40) |
| Disable Verification Requirement | PWD(PIN.SAK) |  |
| Enable  Verification Requirement | ALWAYS |  |
| Get Pin Status | ALWAYS |  |
| Verify | ALWAYS |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (3) |
| Zugriffsregel für logischen LCS „Termination state“ | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | NEVER |  |

* + 1. **⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem Passwortobjekt arbeiten, sind: Activate, Change Reference Data, Deactivate, Delete, Disable Verification Requirement, Enable Verification Requirement, Get Pin Status, Reset Retry Counter, Verify, Terminate
2. Diese Tabellenzeile gilt für den Fall transportStatus gleich Leer-PIN.
3. Diese Tabellenzeile gilt für den Fall transportStatus ungleich Leer-PIN.
   * 1. **⌦** **Card-G2-A\_2576 K\_Initialisierung: CHANGE REFERENCE DATA bei Nutzung der Leer-PIN für PIN.SAK**

* Wenn für PIN.SAK als Transportschutz Leer-PIN verwendet wird, dann DARF PIN.SAK nicht personalisiert werden und es DARF im Zustand *transportStatus* gleich *regularPassword* das Attribut *secret* NICHT mit der Variante Change Reference Data mit P1=1 änderbar sein. Die letzte Anforderung ist herstellerspezifisch umzusetzen.
  + 1. **⌫**
    2. **⌦ Card-G2-A\_3399 K\_Personalisierung: Personalisierte Attribute von MF / PIN.SAK**
* Wenn der Wert des Attributes transportStatus Transport–PIN ist, MÜSSEN bei der Personalisierung von PIN.SAK die in Tab\_gSMC-K\_ObjSys\_097 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 29: Tab\_gSMC-K\_ObjSys\_097 Attribute von MF / PIN.SAK

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| *secret* | PIN-Wert gemäß [gemSpec\_PINPUK\_TI] | wird personalisiert |
| *transportStatus* | Transport-PIN | wird gegebenenfalls personalisiert, siehe Hinweis (41) |

* + 1. **⌫**

1. Für transportStatus wird der Wert „Transport-PIN“ initialisiert. Beispielsweise durch das Kommando Change Reference Data ist es möglich, diesen Wert im Rahmen der Personalisierung auf „regularPassword“ zu setzen.

### MF / PrK.SMC.AUT\_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.AUT\_CVC.E256 gespeichert ist (siehe Kapitel 5.3.12).
    2. **⌦ Card-G2-A\_3332 K\_Initialisierung: Initialisierte Attribute von** MF **/** PrK.SMC.AUT\_CVC.E256
    3. PrK.SMC.AUT\_CVC.E256 MUSS die in Tab\_gSMC-K\_ObjSys\_195 dargestellten Attribute besitzen.

Tabelle 30: Tab\_gSMC-K\_ObjSys\_195 Initialisierte Attribute von MF / PrK.SMC.AUT\_CVC.E256

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| Objekttyp | privates Schlüsselobjekt ELC 256 |  |
| *keyIdentifier* | ‘05’ = 5 |  |
| *privateElcKey* | domainparameter = brainpoolP256r1 |  |
| *privateElcKey* | keyData = AttributNotSet | *wird personalisiert* |
| *keyAvailable* | WildCard |  |
| *numberScenario* | 0 |  |
| *listAlgorithmIdentifier* | alle Werte aus der Menge, siehe [gemSpec\_COS#16.1]  {elcAsynchronAdmin, elcSessionkey4SM} |  |
| *accessRulesSession keys* | Wildcard |  |
| *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=‘81’ | ALWAYS |  |
| Generate Asymmetric Key Pair  P1=´C4´ oder P1=’C0’ | AUT\_CMS OR AUT\_CUP |  |
| General Authenticate | ALWAYS |  |
| Delete | 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 | herstellerspezifisch |  |

* + 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
   * 1. **⌦ Card-G2-A\_3333 K\_Personalisierung: Personalisierte Attribute von MF /** PrK.SMC.AUT\_CVC.E256

Falls das asymmetrische Authentifizierungsverfahren genutzt werden soll, dann MÜSSEN bei der Personalisierung von PrK.SMC.AUT\_CVC.E256 die in Tab\_gSMC-K\_ObjSys\_196 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 31: Tab\_gSMC-K\_ObjSys\_196 Personalisierte Attribute von MF / PrK.SMC.AUT\_CVC.E256

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| *keyAvailable* | True |  |
| privateElcKey | keyData = eine ganze Zahl im Intervall [1, domainParameter.n – 1] |  |

* + 1. **⌫**

### MF / PrK.SMC.AUT\_CVC.E384

* + 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.AUT\_CVC.E384 gespeichert ist (siehe Kapitel 5.3.13).
    2. **⌦ Card-G2-A\_3334 K\_Initialisierung: Initialisierte Attribute von MF / PrK.SMC.AUT\_CVC.E384**
    3. PrK.SMC.AUT\_CVC.E384 MUSS die in Tab\_gSMC-K\_ObjSys\_197 dargestellten Attribute besitzen.
    4. **Tabelle 32: Tab\_gSMC-K\_ObjSys\_197 Initialisierte Attribute von MF / PrK.SMC.AUT\_CVC.E384**

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| Objekttyp | privates Schlüsselobjekt ELC 384 |  |
| *keyIdentifier* | ‘06’ = 6 |  |
| *privateElcKey* | domainparameter = brainpoolP384r1 |  |
| *privateElcKey* | keyData = AttributNotSet |  |
| *keyAvailable* | False |  |
| *numberScenario* | 0 |  |
| *listAlgorithmIdentifier* | alle Werte aus der Menge, siehe [gemSpec\_COS#16.1]  {elcAsynchronAdmin, elcSessionkey4SM} |  |
| *accessRulesSession keys* | irrelevant |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregel für logischen LCS „Operational state (activated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Deacitivate | AUT\_CMS OR AUT\_CUP |  |
| Activate | ALWAYS | herstellerspezifisch ist eine der beiden Varianten erlaubt |
| 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 |  |
| Delete | 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 | herstellerspezifisch |  |

* + 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

### Herstellerspezifische Schlüssel

#### MF / PrK.KONN.AUT.R2048

* + 1. Dieser Schlüssel dient herstellerspezifischen Zwecken und ermöglicht den Aufbau eines TLS-Kanals sowohl client-seitig, als auch server-seitig. Der öffentliche Teil zu diesem priva­ten Schlüssel lässt sich mittels des Kommandos Generate Asymmetric Key Pair (siehe [gemSpec\_COS#14.9.3.4]) auslesen.
    2. Gemäß [TLS#8.1.1] wird für bestimmte Ciphersuites während der Serverauthentisierung eine Entschlüsselung nach [PKCS#1v2.1] Kapitel 7.2 durchgeführt. Deshalb unterstützt dieser Schlüssel den Algorithmus rsaDecipherPKCS1\_V1\_5.
    3. Gemäß [TLS#7.4.8] wird während der Clientauthentisierung eine Signatur nach [PKCS#1v2.1] durchgeführt. Deshalb unterstützt dieser Schlüssel den Algorithmus signPSS.
    4. **⌦ Card-G2-A\_2577 K\_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.AUT.R2048**
* Das Objekt PrK.KONN.AUT.R2048 MUSS die in Tab\_gSMC-K\_ObjSys\_017 dargestellten Werte besitzen.

Tabelle 33: Tab\_gSMC-K\_ObjSys\_017 Initialisierte Attribute von MF / PrK.KONN.AUT.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates RSA Schlüsselobjekt |  |
| *keyIdentifier* | ‘07’ = 7 |  |
| *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]: {  rsaDecipherPKCS1\_V1\_5  sign PKCS1\_V1\_5,  signPSS  } | siehe  Hinweis (45)  Hinweis (46) |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregel für logischen LCS „Operational state (activated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Generate Asymmetric Key Pair  P1=‘84’ oder P1=’80’ | PWD(PIN.Pers) |  |
| Generate Asymmetric Key Pair  P1 =‘81’ | ALWAYS |  |
| PSO CompDigSig | PWD(PIN.AK)  OR PWD(PIN.NK)  OR PWD(PIN.SAK) |  |
| PSO Decipher | PWD(PIN.AK)  OR PWD(PIN.NK)  OR PWD(PIN.SAK) |  |
| Terminate | PWD(PIN.Pers) |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (3) |
| 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. Wird im Rahmen von Serverauthentisierung für RSA–Ciphersuites verwendet.
3. Wird im Rahmen von Client- und Serverauthentisierung von DH–Ciphersuites verwendet.
   * 1. **⌦ Card-G2-A\_3400 K\_Personalisierung: Personalisierte Attribute von MF / PrK.KONN.AUT.R2048**

* Bei der Personalisierung von PrK.KONN.AUT.R2048 MÜSSEN die in Tab\_gSMC-K\_ObjSys\_098 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 34: Tab\_gSMC-K\_ObjSys\_098 Attribute von MF / PrK.KONN.AUT.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| *privateKey* | Moduluslänge 2048 Bit |  |
| *keyAvailable* | true |  |

* + 1. **⌫**

#### MF / PrK.KONN.AUT2.R2048

* + 1. Dieser Schlüssel dient herstellerspezifischen Zwecken und ermöglicht ebenfalls den Aufbau eines TLS-Kanals sowohl client-seitig, als auch server-seitig. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.KONN.AUT.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.
    2. Der öffentliche Teil zu diesem priva­ten Schlüssel lässt sich mittels des Kommandos Generate Asymmetric Key Pair (siehe [gemSpec\_COS#14.9.3.4]) auslesen.
    3. Gemäß [TLS#8.1.1] wird für bestimmte Ciphersuites während der Serverauthentisierung eine Entschlüsselung nach [PKCS#1v2.1] Kapitel 7.2 durchgeführt. Deshalb unterstützt dieser Schlüssel den Algorithmus rsaDecipherPKCS1\_V1\_5.
    4. Gemäß [TLS#7.4.8] wird während der Clientauthentisierung eine Signatur nach [PKCS#1v2.1] durchgeführt. Deshalb unterstützt dieser Schlüssel den Algorithmus signPSS.
    5. **⌦ Card-G2-A\_3442 K\_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.AUT2.R2048**
* Das Objekt PrK.KONN.AUT2.R2048 MUSS die in Tab\_gSMC-K\_ObjSys\_152 dargestellten Werte besitzen.

Tabelle 35: Tab\_gSMC-K\_ObjSys\_152 Initialisierte Attribute von MF / PrK.KONN.AUT2.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates RSA Schlüsselobjekt |  |
| *keyIdentifier* | ‘11’ = 17 |  |
| *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]: {  rsaDecipherPKCS1\_V1\_5  signPKCS1\_V1\_5,  signPSS  } | siehe  Hinweis (45)  Hinweis (46) |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregeln | | |
| *accessRules* | identisch zu PrK.KONN.AUT.R2048 |  |

* + 1. **⌫**

#### MF / PrK.KONN.AUT.R3072

* + 1. Dieser Schlüssel dient herstellerspezifischen Zwecken und ermöglicht ebenfalls den Aufbau eines TLS-Kanals sowohl client- als auch server-seitig. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.KONN.AUT.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.
    2. Gemäß [TLS#8.1.1] wird für bestimmte Ciphersuites während der Serverauthentisierung eine Entschlüsselung nach [PKCS#1v2.1] Kapitel 7.2.2 durchgeführt. Deshalb unterstützt dieser Schlüssel den Algorithmus rsaDecipherPKCS1\_V1\_5.
    3. Gemäß [TLS#7.4.8] wird während der Clientauthentisierung eine Signatur nach [PKCS#1v2.1] durchgeführt. Deshalb unterstützt dieser Schlüssel den Algorithmus signPSS.
    4. **⌦ Card-G2-A\_2578 K\_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.AUT.R3072**
* Das Objekt PrK.KONN.AUT.R3072 MUSS die in Tab\_gSMC-K\_ObjSys\_018 dargestellten Werte besitzen.

Tabelle 36: Tab\_gSMC-K\_ObjSys\_018 Initialisierte Attribute von MF / PrK.KONN.AUT.R3072

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates RSA Schlüsselobjekt |  |
| *keyIdentifier* | ‘0A’ = 10 |  |
| *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]: {  rsaDecipherPKCS1\_V1\_5  signPKCS1\_V1\_5,  signPSS  } | Hinweis (47)  Hinweis (48) |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregeln | | |
| *accessRules* | identisch zu PrK.KONN.AUT.R2048 |  |

* + 1. **⌫**

1. Wird im Rahmen von Serverauthentisierung für RSA-Ciphersuites verwendet.
2. Wird im Rahmen von Client- und Serverauthentisierung von DH-Ciphersuites verwendet.

#### MF / PrK.KONN.AUT.E256

* + 1. Dieser Schlüssel dient herstellerspezifischen Zwecken und ermöglicht ebenfalls den Aufbau eines TLS-Kanals sowohl client-seitig, als auch server-seitig. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.KONN.AUT.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.
    2. **⌦ Card-G2-A\_3443 K\_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.AUT.E256**
* Das Objekt PrK.KONN.AUT.E256 MUSS die in Tab\_gSMC-K\_ObjSys\_178 dargestellten Werte besitzen.

Tabelle 37: Tab\_gSMC-K\_ObjSys\_178 Initialisierte Attribute von MF / PrK.KONN.AUT.E256

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates Schlüsselobjekt, ELC 256 |  |
| *keyIdentifier* | ‘13’ = 19 |  |
| *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]:  { elcSharedSecretCalculation, signECDSA } |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregeln | | |
| *accessRules* | identisch zu PrK.KONN.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

#### MF / PrK.KONN.AUT.E384

* + 1. Dieser Schlüssel dient herstellerspezifischen Zwecken und ermöglicht ebenfalls den Aufbau eines TLS-Kanals sowohl client- als auch server-seitig. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.KONN.AUT.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.
    2. **⌦ Card-G2-A\_2579 K\_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.AUT.E384**
* Das Objekt PrK.KONN.AUT.E384 MUSS die in Tab\_gSMC-K\_ObjSys\_019 dargestellten Werte besitzen.

Tabelle 38: Tab\_gSMC-K\_ObjSys\_019 Initialisierte Attribute von MF / PrK.KONN.AUT.E384

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates Schlüsselobjekt, ELC 384 |  |
| *keyIdentifier* | ‘0E’ = 14 |  |
| *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]:  { elcSharedSecretCalculation, signECDSA } |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregeln | | |
| *accessRules* | identisch zu PrK.KONN.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

#### MF / PrK.KONN.ENC.R2048 (Option\_Erweiterung\_herstellerspezifische\_Schlüssel\_01)

* + 1. Dieser private Schlüssel für die Kryptographie mit RSA dient herstellerspezifischen Zwecken.
    2. Er unterstützt das Entschlüsseln von Daten.
    3. Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos GENERATE ASYMMETRIC KEY PAIR (siehe [gemSpec\_COS#14.9.3.4]) auslesen.
    4. **⌦ Card-G2-A\_3337 K\_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.ENC.R2048 (Option\_Erweiterung\_herstellerspezifische\_Schlüssel\_01)**
    5. PrK.KONN.ENC.R2048 MUSS die in Tab\_gSMC-K\_ObjSys\_198 dargestellten Attribute besitzen.

Tabelle 37: Tab\_gSMC-K\_ObjSys\_198 Initialisierte Attribute von MF / PrK.KONN.ENC.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates RSA Schlüsselobjekt |  |
| *keyIdentifier* | ´09´ = 9 |  |
| *privateKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Moduluslänge 2048 Bit | wird personalisiert |
| *keyAvailable* | WildCard |  |
| *algorithmIdentifier* | alle Werte aus der Menge, siehe [gemSpec\_COS]  { rsaDecipherOaep,  rsaDecipherPKCS1\_V1\_5  } |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregel für logischen LCS „Operational state (activated)” | | |
| *Zugriffsart* | Zugriffsbedingung | Bemerkung |
| GENERATE ASYMMETRIC  KEY PAIR  P1=´C0´ oder  P1=’C4’ | PWD(PIN.Pers) |  |
| GENERATE ASYMMETRIC  KEY PAIR  P1=´81´ | ALWAYS |  |
| PSO Decipher | PWD(PIN.AK) OR PWD(PIN.NK) OR PWD(PIN.SAK) |  |
| PSO Transcipher | PWD(PIN.AK) OR PWD(PIN.NK) OR PWD(PIN.SAK) |  |
| TERMINATE | PWD(PIN.Pers) |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | |
| Zugriffsart | Zugriffsbedingungen | Bemerkungen |
| alle | Herstellerspezifisch | Siehe Hinweis (3) |
| Zugriffsregel für logischen LCS „Termination state“ | | |
| Zugriffsart | Zugriffsbedingungen | Bemerkungen |
| Alle | NEVER |  |

**⌫**

*Hinweis 51: (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*

* + 1. **⌦ Card-G2-A\_3338 K\_Personalisierung: Personalisierte Attribute von MF / PrK.KONN.ENC.R2048 (Option\_Erweiterung\_herstellerspezifische\_Schlüssel\_01)**
* Bei der Personalisierung von PrK.KONN.ENC.R2048 MÜSSEN die in Tab\_gSMC-K\_ObjSys\_199 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 38: Tab\_gSMC-K\_ObjSys\_199 Attribute von MF / PrK.KONN.ENC.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| *privateKey* | Moduluslänge 2048 Bit |  |
| *keyAvailable* | true |  |

* + 1. **⌫**

#### MF / PrK.KONN.ENC2.R2048 (Option\_Erweiterung\_herstellerspezifische\_Schlüssel\_01)

* + 1. Dieser private Schlüssel für die Kryptographie mit RSA dient herstellerspezifischen Zwecken.
    2. Er unterstützt das Entschlüsseln von Daten. Er ist dafür vorgesehen, den Schlüssel PrK.KONN.ENC.R2048 nach Ablauf von dessen Nutzungszeit abzulösen.
    3. Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos GENERATE ASYMMETRIC KEY PAIR (siehe [gemSpec\_COS#14.9.3.4]) auslesen.
    4. **⌦ Card-G2-A\_3339 K\_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.ENC2.R2048 (Option\_Erweiterung\_herstellerspezifische\_Schlüssel\_01)**
    5. PrK.KONN.ENC2.R2048 MUSS die in Tab\_gSMC-K\_ObjSys\_200 dargestellten Attribute besitzen.

Tabelle 39: Tab\_gSMC-K\_ObjSys\_200 Initialisierte Attribute von MF / PrK.KONN.ENC2.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates RSA Schlüsselobjekt |  |
| *keyIdentifier* | ´0D´ = 13 |  |
| *privateKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Moduluslänge 2048 Bit | wird später mit Generate Asymetric Key Pair erzeugt |
| *keyAvailable* | False |  |
| *algorithmIdentifier* | alle Werte aus der Menge, siehe [gemSpec\_COS]  { rsaDecipherOaep,  rsaDecipherPKCS1\_V1\_5  } |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregeln | | |
| *accessRules* | Identisch zu PrK.KONN.ENC.R2048 |  |

**⌫**

*Hinweis 51: (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 / PrK.KONN.ENC.R3072 (Option\_Erweiterung\_herstellerspezifische\_Schlüssel\_01)

* + 1. Dieser private Schlüssel für die Kryptographie mit RSA dient herstellerspezifischen Zwecken.
    2. Er unterstützt das Entschlüsseln von Daten. Er ist dafür vorgesehen, die Schlüssel PrK.KONN.ENC.R2048 bzw. PrK.KONN.ENC2.R2048 nach Ablauf von deren Nutzungszeit abzulösen.
    3. Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos GENERATE ASYMMETRIC KEY PAIR (siehe [gemSpec\_COS#14.9.3.4]) auslesen.
    4. **⌦ Card-G2-A\_3345 K\_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.ENC.R3072 (Option\_Erweiterung\_herstellerspezifische\_Schlüssel\_01)**
    5. PrK.KONN.ENC.R3072 MUSS die in Tab\_gSMC-K\_ObjSys\_201 dargestellten Attribute besitzen.

Tabelle 40: Tab\_gSMC-K\_ObjSys\_201 Initialisierte Attribute von MF / PrK.KONN.ENC.R3072

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates RSA Schlüsselobjekt |  |
| *keyIdentifier* | ´0F´ = 15 |  |
| *privateKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Moduluslänge 3072 Bit | wird später mit Generate Asymetric Key Pair erzeugt |
| *keyAvailable* | False |  |
| *algorithmIdentifier* | alle Werte aus der Menge, siehe [gemSpec\_COS]  { rsaDecipherOaep,  rsaDecipherPKCS1\_V1\_5  } |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregeln | | |
| *accessRules* | Identisch zu PrK.KONN.ENC.R2048 |  |

**⌫**

#### MF / PrK.KONN.TLS.R2048 (Option\_Erweiterung\_herstellerspezifische\_Schlüssel\_01)

* + 1. Dieser private Schlüssel für die Kryptographie mit RSA dient herstellerspezifischen Zwecken.
    2. Er unterstützt das Signieren und das Entschlüsseln von Daten. Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos GENERATE ASYMMETRIC KEY PAIR (siehe [gemSpec\_COS#14.9.3.4]) auslesen.
    3. **⌦ Card-G2-A\_3372 K\_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.TLS.R2048 (Option\_Erweiterung\_herstellerspezifische\_Schlüssel\_01)**
    4. PrK.KONN.TLS.R2048 MUSS die in Tab\_gSMC-K\_ObjSys\_202 dargestellten Attribute besitzen.

Tabelle 41: Tab\_gSMC-K\_ObjSys\_202 Initialisierte Attribute von MF / PrK.KONN.TLS.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates RSA Schlüsselobjekt |  |
| *keyIdentifier* | ´10´ = 16 |  |
| *privateKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichendfür einen Schlüssel mit Moduluslänge 2048 Bit | wird personalisiert |
| *keyAvailable* | WildCard |  |
| *algorithmIdentifier* | alle Werte aus der Menge, siehe [gemSpec\_COS]  { signPSS,  signPKCS1\_V1\_5,  rsaDecipherOaep,  rsaDecipherPKCS1\_V1\_5  } |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregel für logischen LCS „Operational state (activated)” | | |
| *Zugriffsart* | Zugriffsbedingung | Bemerkung |
| GENERATE ASYMMETRIC  KEY PAIR  P1=´C0´ oder  P1=’C4’ | PWD(PIN.Pers) |  |
| GENERATE ASYMMETRIC  KEY PAIR  P1=´81´ | ALWAYS |  |
| PSO CompDigSig | PWD(PIN.AK) OR PWD(PIN.NK) OR PWD(PIN.SAK) |  |
| PSO Decipher | PWD(PIN.AK) OR PWD(PIN.NK) OR PWD(PIN.SAK) |  |
| TERMINATE | PWD(PIN.Pers) |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | |
| Zugriffsart | Zugriffsbedingungen | Bemerkungen |
| alle | Herstellerspezifisch | Siehe Hinweis (3) |
| Zugriffsregel für logischen LCS „Termination state“ | | |
| Zugriffsart | Zugriffsbedingungen | Bemerkungen |
| Alle | NEVER |  |

**⌫**

*Hinweis 52: (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*

* + 1. **⌦ Card-G2-A\_3376 K\_Personalisierung: Personalisierte Attribute von MF / PrK.KONN.TLS.R2048 (Option\_Erweiterung\_herstellerspezifische\_Schlüssel\_01)**
* Bei der Personalisierung von PrK.KONN.TLS.R2048 MÜSSEN die in Tab\_gSMC-K\_ObjSys\_203 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 42: Tab\_gSMC-K\_ObjSys\_203 Attribute von MF / PrK.KONN.TLS.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| *privateKey* | Moduluslänge 2048 Bit |  |
| *keyAvailable* | true |  |

* + 1. **⌫**

#### MF / PrK.KONN.TLS2.R2048 (Option\_Erweiterung\_herstellerspezifische\_Schlüssel\_01)

* + 1. Dieser private Schlüssel für die Kryptographie mit RSA dient herstellerspezifischen Zwecken.
    2. Er unterstützt das Signieren und das Entschlüsseln von Daten. Er ist dafür vorgesehen, den Schlüssel PrK.KONN.TLS.R2048 nach Ablauf von dessen Nutzungszeit abzulösen.
    3. Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos GENERATE ASYMMETRIC KEY PAIR (siehe [gemSpec\_COS#14.9.3.4]) auslesen.
    4. **⌦ Card-G2-A\_3377 K\_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.TLS2.R2048 (Option\_Erweiterung\_herstellerspezifische\_Schlüssel\_01)**
    5. PrK.KONN.TLS2.R2048 MUSS die in Tab\_gSMC-K\_ObjSys\_204 dargestellten Attribute besitzen.

Tabelle 43: Tab\_gSMC-K\_ObjSys\_204 Initialisierte Attribute von MF / PrK.KONN.TLS2.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates RSA Schlüsselobjekt |  |
| *keyIdentifier* | ‘02‘ = 2 |  |
| *privateKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichendfür einen Schlüssel mit Moduluslänge 2048 Bit | wird später mit Generate Asymetric Key Pair erzeugt |
| *keyAvailable* | False |  |
| *algorithmIdentifier* | alle Werte aus der Menge, siehe [gemSpec\_COS]  { signPSS,  signPKCS1\_V1\_5,  rsaDecipherOaep,  rsaDecipherPKCS1\_V1\_5  } |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregeln | | |
| *accessRules* | Identisch zu PrK.KONN.TLS.R2048 |  |

**⌫**

#### MF / PrK.KONN.TLS.R3072 (Option\_Erweiterung\_herstellerspezifische\_Schlüssel\_01)

* + 1. Dieser private Schlüssel für die Kryptographie mit RSA dient herstellerspezifischen Zwecken.
    2. Er unterstützt das Signieren und das Entschlüsseln von Daten. Er ist dafür vorgesehen, die Schlüssel PrK.KONN.TLS.R2048 bzw. PrK.KONN.TLS2.R2048 nach Ablauf ihrer Nutzungszeit abzulösen.
    3. Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos GENERATE ASYMMETRIC KEY PAIR (siehe [gemSpec\_COS#14.9.3.4]) auslesen.
    4. **⌦ Card-G2-A\_3378 K\_Initialisierung: Initialisierte Attribute von MF / PrK.KONN.TLS.R3072 (Option\_Erweiterung\_herstellerspezifische\_Schlüssel\_01)**
    5. PrK.KONN.TLS.R3072 MUSS die in Tab\_gSMC-K\_ObjSys\_205 dargestellten Attribute besitzen.

Tabelle 44: Tab\_gSMC-K\_ObjSys\_205 Initialisierte Attribute von MF / PrK.KONN.TLS.R3072

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates RSA Schlüsselobjekt |  |
| *keyIdentifier* | ´15´ = 21 |  |
| *privateKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichendfür einen Schlüssel mit Moduluslänge 3072 Bit | wird später mit Generate Asymetric Key Pair erzeugt |
| *keyAvailable* | False |  |
| *algorithmIdentifier* | alle Werte aus der Menge, siehe [gemSpec\_COS]  { signPSS,  signPKCS1\_V1\_5,  rsaDecipherOaep,  rsaDecipherPKCS1\_V1\_5  } |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregeln | | |
| *accessRules* | Identisch zu PrK.KONN.TLS.R2048 |  |

**⌫**

#### MF / EF.PuK.KONN.SIG.R4096 (Option\_Erweiterung\_herstellerspezifische\_Schlüssel\_01)

* + 1. Diese Datei dient herstellerspezifischen Zwecken. Sie kann einen öffentlichen Schlüssel des Konnektorherstellers enthalten. Er kann vom Konnektor ausgelesen werden, um extern erhaltene Informationen hinsichtlich ihrer Integrität zu verifizieren.
    2. **⌦ Card-G2-A\_3379 K\_Initialisierung: Initialisierte Attribute von MF / EF.PuK.KONN.SIG.R4096 (Option\_Erweiterung\_herstellerspezifische\_Schlüssel\_01)**
    3. EF.PuK.KONN.SIG.R4096 MUSS die in Tab\_gSMC-K\_ObjSys\_206 dargestellten Attribute besitzen.

Tabelle 45: Tab\_gSMC-K\_ObjSys\_206 Initialisierte Attribute von MF / EF.PuK.KONN.SIG.R4096

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attribute | | Wert | Bemerkung | |
| Objekttyp | | transparentes Elementary File |  | |
| *fileIdentifier* | | ´2F 16´ |  | |
| *shortFileIdentifier* | | - |  | |
| *numberOfOctet* | | ´0210´ Oktett = 528 Oktett |  | |
| *positionLogicalEndOfFile* | | WildCard | wird personalisiert | |
| *flagTransactionMode* | | False |  | |
| *flagCheckSum* | | True |  | |
| *lifeCycleStatus* | | „Operational state (activated)“ |  | |
| *shareable* | | True |  | |
| *body* | | kein Inhalt | Wird personalisiert | |
| Zugriffsregel für logischen LCS „Operational state (activated)” | | | | |
| *Zugriffsart* | | Zugriffsbedingung | Bemerkung | |
| READ BINARY | | ALWAYS |  | |
| ERASE BINARY  SET LOGICAL EOF  UPDATE BINARY  WRITE BINARY | | AUT\_CMS OR AUT\_CUP |  | |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | | | |
| Zugriffsart | Zugriffsbedingungen | | | Bemerkungen |
| alle | Herstellerspezifisch | | | Siehe Hinweis (3) |
| Zugriffsregel für logischen LCS „Termination state“ | | | | |
| Zugriffsart | Zugriffsbedingungen | | | Bemerkungen |
| Alle | NEVER | | |  |

**⌫**

*Hinweis 53: Kommandos, die gemäß [gemSpec\_COS] mit einem transparenten EF arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Set Logical Eof, Update Binary, Terminate, Write Binary.*

* + 1. **⌦ Card-G2-A\_3380 K\_Personalisierung: Personalisierte Attribute von MF / EF.PuK.KONN.SIG.R4096 (Option\_Erweiterung\_herstellerspezifische\_Schlüssel\_01)**
* Wenn EF.PuK.KONN.SIG.R4096 personalisiert wird,MÜSSEN die in Tab\_gSMC-K\_ObjSys\_207 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 46: Tab\_gSMC-K\_ObjSys\_207 Attribute von MF / EF.PuK.KONN.SIG.R4096

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| *positionLogicalEndOfFil*e | Zahl der tatsächlich belegten Oktette |  |
| *body* | Öffentlicher Schlüssel des Konnektorherstellers mit Moduluslänge 4096 Bit  codiert gemäß [PKCS#1v2.1#A.1.1] |  |
| *body*  Option\_Erstellung \_von\_Testkarten | Öffentlicher Schlüssel des Konnektorherstellers mit Moduluslänge 4096 Bit  codiert gemäß [PKCS#1v2.1#A.1.1] |  |

* + 1. **⌫**

#### MF / PrK.SDS.R2048 (Option\_Erweiterung\_herstellerspezifische\_Schlüssel\_01)

* + 1. Dieser private Schlüssel für die Kryptographie mit RSA dient herstellerspezifischen Zwecken.
    2. Er unterstützt das Signieren und das Entschlüsseln von Daten.
    3. Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos GENERATE ASYMMETRIC KEY PAIR (siehe [gemSpec\_COS#14.9.3.4]) auslesen.
    4. **⌦ Card-G2-A\_3381 K\_Initialisierung: Initialisierte Attribute von MF / PrK.SDS.R2048 (Option\_Erweiterung\_herstellerspezifische\_Schlüssel\_01)**
    5. PrK.SDS.R2048 MUSS die in Tab\_gSMC-K\_ObjSys\_208 dargestellten Attribute besitzen.

Tabelle 47: Tab\_gSMC-K\_ObjSys\_208 Initialisierte Attribute von MF / PrK.SDS.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates RSA Schlüsselobjekt |  |
| *keyIdentifier* | ´16´ = 22 |  |
| *privateKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Moduluslänge 2048 Bit | wird personalisiert |
| *keyAvailable* | WildCard |  |
| *algorithmIdentifier* | alle Werte aus der Menge, siehe [gemSpec\_COS]  { signPSS,  signPKCS1\_V1\_5,  rsaDecipherOaep,  rsaDecipherPKCS1\_V1\_5  } |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregel für logischen LCS „Operational state (activated)” | | |
| *Zugriffsart* | Zugriffsbedingung | Bemerkung |
| GENERATE ASYMMETRIC  KEY PAIR  P1=´C0´ oder  P1=’C4’ | PWD(PIN.Pers) |  |
| GENERATE ASYMMETRIC  KEY PAIR  P1=´81´ | ALWAYS |  |
| PSO CompDigSig | PWD(PIN.NK) |  |
| PSO Decipher | PWD(PIN.NK) |  |
| PSO Transcipher | PWD(PIN.NK) |  |
| TERMINATE | PWD(PIN.Pers) |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | |
| Zugriffsart | Zugriffsbedingungen | Bemerkungen |
| Alle | Herstellerspezifisch | Siehe Hinweis (3) |
| Zugriffsregel für logischen LCS „Termination state“ | | |
| Zugriffsart | Zugriffsbedingungen | Bemerkungen |
| Alle | NEVER |  |

**⌫**

*Hinweis 54: (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*

* + 1. **⌦ Card-G2-A\_3382 K\_Personalisierung: Personalisierte Attribute von MF / PrK.SDS.R2048 (Option\_Erweiterung\_herstellerspezifische\_Schlüssel\_01)**
* Bei der Personalisierung von PrK.SDS.R2048 MÜSSEN die in Tab\_gSMC-K\_ObjSys\_209 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 48: Tab\_gSMC-K\_ObjSys\_209 Attribute von MF / PrK.SDS.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| *privateKey* | Moduluslänge 2048 Bit |  |
| *keyAvailable* | true |  |

* + 1. **⌫**

#### MF / PrK.SDS2.R2048 (Option\_Erweiterung\_herstellerspezifische\_Schlüssel\_01)

* + 1. Dieser private Schlüssel für die Kryptographie mit RSA dient herstellerspezifischen Zwecken. Er unterstützt das Signieren und das Entschlüsseln von Daten. Er ist dafür vorgesehen, den Schlüssel PrK.SDS.R2048 nach Ablauf von dessen Nutzungszeit abzulösen.
    2. Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos GENERATE ASYMMETRIC KEY PAIR (siehe [gemSpec\_COS#14.9.3.4]) auslesen.
    3. **⌦ Card-G2-A\_3383 K\_Initialisierung: Initialisierte Attribute von MF / PrK.SDS2.R2048 (Option\_Erweiterung\_herstellerspezifische\_Schlüssel\_01)**
    4. PrK.SDS2.R2048 MUSS die in Tab\_gSMC-K\_ObjSys\_210 dargestellten Attribute besitzen.

Tabelle 49: Tab\_gSMC-K\_ObjSys\_210 Initialisierte Attribute von MF / PrK.SDS2.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates RSA Schlüsselobjekt |  |
| *keyIdentifier* | ´19´ = 25 |  |
| *privateKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Moduluslänge 2048 Bit | wird später mit Generate Asymetric Key Pair erzeugt |
| *keyAvailable* | False |  |
| *algorithmIdentifier* | alle Werte aus der Menge, siehe [gemSpec\_COS]  { signPSS,  signPKCS1\_V1\_5,  rsaDecipherOaep,  rsaDecipherPKCS1\_V1\_5  } |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregeln | | |
| *accessRules* | Identisch zu PrK.SDS.R2048 |  |

**⌫**

#### MF / PrK.SDS.R3072 (Option\_Erweiterung\_herstellerspezifische\_Schlüssel\_01)

* + 1. Dieser private Schlüssel für die Kryptographie mit RSA dient herstellerspezifischen Zwecken. Er unterstützt das Signieren und das Entschlüsseln von Daten. Er ist dafür vorgesehen, die Schlüssel PrK.SDS.R2048 bzw. PrK.SDS2.R2048 nach Ablauf von deren Nutzungszeit abzulösen.
    2. Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos GENERATE ASYMMETRIC KEY PAIR (siehe [gemSpec\_COS#14.9.3.4]) auslesen.
    3. **⌦ Card-G2-A\_3384 K\_Initialisierung: Initialisierte Attribute von MF / PrK.SDS.R3072 (Option\_Erweiterung\_herstellerspezifische\_Schlüssel\_01)**
    4. PrK.SDS.R3072 MUSS die in Tab\_gSMC-K\_ObjSys\_211 dargestellten Attribute besitzen.

Tabelle 50: Tab\_gSMC-K\_ObjSys\_211 Initialisierte Attribute von MF / PrK.SDS.R3072

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates RSA Schlüsselobjekt |  |
| *keyIdentifier* | ´1A´ = 26 |  |
| *privateKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Moduluslänge 3072 Bit | wird später mit Generate Asymetric Key Pair erzeugt |
| *keyAvailable* | False |  |
| *algorithmIdentifier* | alle Werte aus der Menge, siehe [gemSpec\_COS]  { signPSS,  signPKCS1\_V1\_5,  rsaDecipherOaep,  rsaDecipherPKCS1\_V1\_5  } |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregeln | | |
| *accessRules* | Identisch zu PrK.SDS.R2048 |  |

**⌫**

#### MF / PrK.GP.R2048

* + 1. Dieser private Schlüssel für die Kryptographie mit RSA dient herstellerspezifischen Zwecken. Er unterstützt das Signieren und das Entschlüsseln von Daten. Der zugehörige öffentliche Schlüssel ist PuK.GP.R2048 (siehe Kapitel 5.3.20.17). Er lässt sich auch mittels des Kommandos Generate Asymmetric Key Pair (siehe [gemSpec\_COS#14.9.3.4]) auslesen.
    2. **⌦ Card-G2-A\_2580 K\_Initialisierung: Initialisierte Attribute von MF / PrK.GP.R2048**
* Das Objekt PrK.GP.R2048 MUSS die in Tab\_gSMC-K\_ObjSys\_020 dargestellten Werte besitzen.

Tabelle 39: Tab\_gSMC-K\_ObjSys\_020 Initialisierte Attribute von MF / PrK.GP.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates RSA Schlüsselobjekt |  |
| *keyIdentifier* | ‘0C’ = 12 |  |
| *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]: {  signPSS,  rsaDecipherOaep,  rsaDecipherPKCS1\_V1\_5  } |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregel für logischen LCS „Operational state (activated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Generate Asymmetric Key Pair  P1=‘84’ oder P1=’80’ | PWD(PIN.Pers) |  |
| Generate Asymmetric Key Pair  P1=‘81’ | ALWAYS |  |
| PSO CompDigSig | PWD(PIN.AK)  OR PWD(PIN.NK)  OR PWD(PIN.SAK) |  |
| PSO Decipher | PWD(PIN.AK)  OR PWD(PIN.NK)  OR PWD(PIN.SAK) |  |
| PSO Transcipher | PWD(PIN.AK)  OR PWD(PIN.NK)  OR PWD(PIN.SAK) |  |
| Terminate | PWD(PIN.Pers) |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (3) |
| 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
   * 1. **⌦ Card-G2-A\_3401 K\_Personalisierung: Personalisierte Attribute von MF / PrK.GP.R2048**

* Bei der Personalisierung von PrK.GP.R2048 MÜSSEN die in Tab\_gSMC-K\_ObjSys\_101 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 40: Tab\_gSMC-K\_ObjSys\_101 Attribute von MF / PrK.GP.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| *privateKey* | Moduluslänge 2048 Bit |  |
| *keyAvailable* | true |  |

* + 1. **⌫**

#### MF / PuK.GP.R2048

* + 1. Dieses Objekt enthält den öffentlichen Schlüssel für die Kryptographie mit RSA zu PrK.GP.R2048 (siehe Kapitel 5.3.20.16). Der öffentliche Schlüssel dient der Verschlüsselung von Daten.
    2. **⌦ Card-G2-A\_2585 K\_Initialisierung: Initialisierte Attribute von MF / PuK.GP.R2048**
* Das Objekt PuK.GP.R2048 MUSS die in Tab\_gSMC-K\_ObjSys\_027 dargestellten Werte besitzen.

Tabelle 41: Tab\_gSMC-K\_ObjSys\_027 Initialisierte Attribute von MF / PuK.GP.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | öffentliches RSA Verschlüsselungsobjekt |  |
| *keyIdentifier* | '00000000000000000000001C’ |  |
| *privateKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Moduluslänge 2048 Bit | wird personalisiert |
| *oid* | id-RSAES-OAEP = {1.2.840.113549.1.1.7} = ‘2A864886F70d010107’ |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| PSO Encipher | ALWAYS |  |
| Terminate | PWD(PIN.Pers) |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (3) |
| Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | NEVER |  |

* + 1. **⌫**

1. Kommandos, die gemäß [gemSpec\_COS#8.6.4.3] mit einem öffentlichen Verschlüsselungsobjekt arbeiten sind: PSO Encipher, Terminate
   * 1. **⌦ Card-G2-A\_3402 K\_Personalisierung: Personalisierte Attribute von MF / PuK.GP.R2048**

* Bei der Personalisierung von PuK.GP.R2048 MÜSSEN die in Tab\_gSMC-K\_ObjSys\_104 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 42: Tab\_gSMC-K\_ObjSys\_104 Attribute von MF / PuK.GP.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| *publicKey* | Moduluslänge 2048 Bit |  |

* + 1. **⌫**

#### MF / PrK.GP2.R2048

* + 1. Dieser private Schlüssel für die Kryptographie mit RSA dient ebenfalls herstellerspezifischen Zwecken. Er unterstützt das Signieren und das Entschlüsseln von Daten. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.GP.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.
    2. Der zugehörige öffentliche Schlüssel ist PuK.GP.R2048. Er lässt sich mittels des Kommandos Generate Asymmetric Key Pair (siehe [gemSpec\_COS#14.9.3.4]) auslesen.
    3. **⌦ Card-G2-A\_3444 K\_Initialisierung: Initialisierte Attribute von MF / PrK.GP2.R2048**
* Das Objekt PrK.GP2.R2048 MUSS die in Tab\_gSMC-K\_ObjSys\_153 dargestellten Werte besitzen.

Tabelle 43: Tab\_gSMC-K\_ObjSys\_153 Initialisierte Attribute von MF / PrK.GP2.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates Schlüsselobjekt, RSA 2048 |  |
| *keyIdentifier* | ‘0B’ = 11 |  |
| *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]: {  signPSS,  rsaDecipherOaep,  rsaDecipherPKCS1\_V1\_5  } |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregeln | | |
| *accessRules* | identisch zu PrK.GP.R2048 |  |

* + 1. **⌫**

#### MF / PrK.GP.R3072

* + 1. Dieser private Schlüssel für die Kryptographie mit RSA dient ebenfalls herstellerspezifischen Zwecken. Er unterstützt das Signieren und das Entschlüsseln von Daten. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.GP.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.
    2. Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos Generate Asymmetric Key Pair (siehe [gemSpec\_COS#14.9.3.4]) auslesen.
    3. **⌦ Card-G2-A\_2581 K\_Initialisierung: Initialisierte Attribute von MF / PrK.GP.R3072**
* Das Objekt PrK.GP.R3072 MUSS die in Tab\_gSMC-K\_ObjSys\_021 dargestellten Werte besitzen.

Tabelle 44: Tab\_gSMC-K\_ObjSys\_021 Initialisierte Attribute von MF / PrK.GP.R3072

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates Schlüsselobjekt, RSA 3072 |  |
| *keyIdentifier* | ‘12’ = 18 |  |
| *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]: {  signPSS,  rsaDecipherOaep,  rsaDecipherPKCS1\_V1\_5  } |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregeln | | |
| *accessRules* | identisch zu PrK.GP.R2048 |  |

* + 1. **⌫**

#### MF / PrK.GP.E256

* + 1. Dieser private Schlüssel für die Kryptographie mit RSA dient ebenfalls herstellerspezifischen Zwecken. Er unterstützt das Signieren und das Entschlüsseln von Daten. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.GP.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.
    2. Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos Generate Asymmetric Key Pair (siehe [gemSpec\_COS#14.9.3.4]) auslesen.
    3. **⌦ Card-G2-A\_3446 K\_Initialisierung: Initialisierte Attribute von MF / PrK.GP.E256**
* Das Objekt PrK.GP.E256 MUSS die in Tab\_gSMC-K\_ObjSys\_179 dargestellten Werte besitzen.

Tabelle 45: Tab\_gSMC-K\_ObjSys\_179 Initialisierte Attribute von MF / PrK.GP.E256

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates Schlüsselobjekt, ELC 256 |  |
| *keyIdentifier* | ‘08’ = 8 |  |
| *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]:  {elcSharedSecretCalculation, signECDSA } |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregeln | | |
| *accessRules* | identisch zu PrK.GP.R2048 |  |

* + 1. **⌫**

#### MF / PrK.GP.E384

* + 1. Dieser private Schlüssel für die Kryptographie mit RSA dient ebenfalls herstellerspezifischen Zwecken. Er unterstützt das Signieren und das Entschlüsseln von Daten. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.GP.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.
    2. Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos Generate Asymmetric Key Pair (siehe [gemSpec\_COS#14.9.3.4]) auslesen.
    3. **⌦ Card-G2-A\_2582 K\_Initialisierung: Initialisierte Attribute von MF / PrK.GP.E384**
* Das Objekt PrK.GP.E384 MUSS die in Tab\_gSMC-K\_ObjSys\_022 dargestellten Werte besitzen.

Tabelle 46: Tab\_gSMC-K\_ObjSys\_022 Initialisierte Attribute von MF / PrK.GP.E384

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates Schlüsselobjekt, ELC 384 |  |
| *keyIdentifier* | ‘17’ = 23 |  |
| *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]:  {elcSharedSecretCalculation, signECDSA } |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregeln | | |
| *accessRules* | identisch zu PrK.GP.R2048 |  |

* + 1. **⌫**

### 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.

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

* + 1. Dieses Objekt enthält den öffentlichen Schlüssel der Root-CA, welcher an der Wurzel der der CVC.E256-Hierarchie steht. Er wird zur Prüfung von CV-Zertifikaten der zweiten Ebene von Karten der Generation 2 unter Nutzung elliptischer Kryptographie benötigt.
    2. **⌦ Card-G2-A\_2583 K\_Initialisierung: Initialisierte Attribute von MF / PuK.RCA.CS.E256**
* Das Objekt PuK.RCA.CS.E256 MUSS die in Tab\_gSMC-K\_ObjSys\_024 dargestellten Werte besitzen.

Tabelle 47: Tab\_gSMC-K\_ObjSys\_024 Initialisierte Attribute von MF / PuK.RCA.CS.E256

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | öffentliches 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) |  |
| CHAT | * OIDflags     = oid\_cvc\_fl\_ti * flagList       = ‘FF 0084 2006 07D8’ | siehe Hinweis (54) |
| *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#4.5] |  |
| Für Echtkarten MÜSSEN die nachfolgenden Attribute mit den unten angegebenen Werten initialisiert werden.  Für Option\_Erstellung\_von\_Testkarten MÜSSEN die nachfolgenden Attribute entweder mit den unten angegebenen Werten oder mit Wildcard oder AttributeNotSet initialisiert werden. | | |
| *oid* | ecdsa-with-SHA256  ‘2A8648CE3D040302’ = {1.2.840.10045.4.3.2} |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *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 (55) |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (3) |
| Zugriffsregel für logischen LCS „Termination state“ | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | NEVER |  |

* + 1. **⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem öffentlichen Signaturprüfobjekt arbeiten sind: PSO Verify Certificate, Terminate
2. 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.
3. Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap. 5.10.
   * 1. **⌦ Card-G2-A\_3262 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-K\_ObjSys\_191 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.
* Wenn die restlichen Attribute von PuK.RCS.CS.E256 mit Wildcard oder AttributeNotSet initialisiert wurden, MÜSSEN sie gemäß den Vorgaben in der Initialisierungstabelle Tab\_gSMC-K\_ObjSys\_024 personalisiert werden.

Tabelle 48: Tab\_gSMC-K\_ObjSys\_191 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 07D8’ |  |
| *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-K betrifft ein Administrationssystem (i.A. ein Kartenmanagementsystem (CMS)) zur Administration der gSMC-K.
    2. Die Administration einer gSMC-K erfordert den Aufbau eines kryptographisch gesicherten Kommunikationskanals (Trusted Channel). In diesem Kapitel werden Schlüssel beschrieben, die den Aufbau eines solchen Trusted Channels mittels asymmetrischer Verfahren ermöglichen. Die Schlüssel zum Aufbau mittels symmetrischer Verfahren werden in 5.3.23 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 Smart Card und (PrK.Admin, PuK.Admin) das Schlüsselpaar des administrierenden Systems, dann ist es erforderlich, dass die Smart Card PuK.Admin kennt und das administrierende System PuK.ICC kennt.
    4. Während die Schlüsselpaare auf Smart Cards typischerweise kartenindividuell sind, so ist es denkbar, dass mit einem Schlüsselpaar eines administrierenden Systems genau eine, oder mehrere oder alle Smart Cards administriert werden. Das Sicherheitskonzept des administrierenden Systems erscheint die geeignete Stelle zu sein um eine Variante auszuwählen.

#### 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\_2998 K\_Initialisierung: Initialisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256**
* PuK.RCA.ADMINCMS.CS.E256 MUSS die in Tab\_gSMC-K\_ObjSys\_085 dargestellten Attribute besitzen.

Tabelle 49: Tab\_gSMC-K\_ObjSys\_085 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 (57) | |
| *expirationDate* | Identisch zu „expirationDate“ von PuK.RCA.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 (58) |
| 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: 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 Kapitel 5.10
   * 1. **⌦ Card-G2-A\_3403 K\_Personalisierung: Personalisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256**
4. Bei der Personalisierung von PuK.RCA.ADMINCMS.CS.E256 MÜSSEN die in Tab\_gSMC-K\_ObjSys\_108 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.
5. 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-K\_ObjSys\_085 personalisiert werden.

Tabelle 50: Tab\_gSMC-K\_ObjSys\_108 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-K betrifft ein Administrationssystem (i.A. ein Kartenmanagementsystem (CMS)) zur Administration der gSMC-K.
    2. Die Administration einer gSMC-K erfordert den Aufbau eines kryptographisch gesicherten Kommunikationskanals (Trusted Channel). In diesem Kapitel werden Schlüssel beschrieben, die den Aufbau eines solchen Trusted Channels mittels symmetrischer Verfahren ermöglichen. Die Schlüssel zum Aufbau mittels asymmetrischer Verfahren werden in 5.3.22 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. Wenn die symmetrischen Schlüssel (SK.CMS und SK.CUP) für die Authentifizierung des Kartenadministrationssystems genutzt werden, dann MÜSSEN sie kartenindividuell personalisiert werden, so dass mit einem Schlüssel eines administrierenden Systems genau eine gSMC-K administriert werden kann.
    5. Bei der Personalisierung sind nur die Schlüssel zu personalisieren, die tatsächlich benötigt werden.

#### MF /. SK.CMS.AES128

SK.CMS.AES128 (optional) ist der geheime AES-Schlüssel für die Durchführung des Konnektor/CMS-Authentisie­rungs­verfahrens mit Aufbau eines Trusted Channel. Die nachfolgende Tabelle Tab\_gSMC-K\_ObjSys\_030 zeigt die Eigenschaften des Schlüssels.

* + 1. **⌦ Card-G2-A\_2588 K\_Initialisierung: Initialisierte Attribute von** **MF / SK.CMS.AES128**
* Das Objekt SK.CMS.AES128 MUSS die in Tab\_gSMC-K\_ObjSys\_030 dargestellten Werte besitzen.

Tabelle 51: Tab\_gSMC-K\_ObjSys\_030 Initialisierte Attribute von MF / SK.CMS.AES128

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | Symmetrisches Authentisierungsobjekt |  |
| *keyType* | AES-128 |  |
| *keyIdentifier* | ‘14’ = 20 |  |
| *encKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 128 Bit | wird personalisiert |
| *macKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 128 Bit | wird personalisiert |
| *numberScenario* | 0 |  |
| *algorithmIdentifier* | aesSessionkey4SM, siehe [gemSpec\_COS] |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *accessRulesSessionkeys* | irrelevant |  |
| Zugriffsregeln | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Mutual Authenticate | PWD(PIN.AK)  OR PWD(PIN.NK)  OR PWD(PIN.SAK) |  |
| Delete | AUT\_CMS OR AUT\_CUP | siehe Hinweis (60) |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (3) |
| Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet | | |
| 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- bzw. CUP-Schlüssels ausführbar, siehe Kapitel 5.10.
   * 1. **⌦ Card-G2-A\_3404 K\_Personalisierung: Personalisierte Attribute von** **MF / SK.CMS.AES128**

* Falls das symmetrische Authentifizierungsverfahren genutzt werden soll, dann MÜSSEN bei der Personalisierung von SK.CMS.AES128 die in Tab\_gSMC-K\_ObjSys\_110 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 52: Tab\_gSMC-K\_ObjSys\_110 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 ist der geheime AES-Schlüssel für die Durchführung des Konnektor/CMS-Authentisie­rungs­verfahrens mit Aufbau eines Trusted Channel. Die nachfolgende Tabelle Tab\_gSMC-K\_ObjSys\_031 zeigt die Eigenschaften des Schlüssels.
    2. **⌦ Card-G2-A\_2589 K\_Initialisierung: Initialisierte Attribute von MF / SK.CMS.AES256**
* Das Objekt SK.CMS.AES256 MUSS die in Tab\_gSMC-K\_ObjSys\_031 dargestellten Werte besitzen.

Tabelle 53: Tab\_gSMC-K\_ObjSys\_031 Initialisierte Attribute von MF / SK.CMS.AES256

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | Symmetrisches Authentisierungsobjekt |  |
| *keyType* | AES-256 |  |
| *keyIdentifier* | ‘18’ = 24 |  |
| *encKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 256 Bit | wird personalisiert |
| *macKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 256 Bit | wird personalisiert |
| *numberScenario* | 0 |  |
| *algorithmIdentifier* | aesSessionkey4SM, siehe [gemSpec\_COS] |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *accessRulesSessionkeys* | irrelevant |  |
| 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\_3405 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-K\_ObjSys\_111 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 54: Tab\_gSMC-K\_ObjSys\_111 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-K bezüglich der Zertifikate zu erlauben.
    2. **⌦ Card-G2-A\_3206 K\_Initialisierung: Initialisierte Attribute von MF / SK.CUP.AES128**
* SK.CUP.AES128 MUSS die in Tab\_gSMC-K\_ObjSys\_154 dargestellten Initialisierten Attribute besitzen.

Tabelle 55: Tab\_gSMC-K\_ObjSys\_154 Initialisierte Attribute von MF / SK.CUP.AES128

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | Symmetrisches Authentisierungsobjekt |  |
| *keyType* | AES-128 |  |
| *keyIdentifier* | ’03’ = 3 |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *encKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 128 Bit | wird personalisiert |
| *macKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 128 Bit | wird personalisiert |
| *numberScenario* | 0 |  |
| *algorithmIdentifier* | aesSessionkey4SM, siehe [gemSpec\_COS] |  |
| *accessRulesSessionkeys* | irrelevant |  |
| Zugriffsregeln | | |
| *accessRules* | identisch zu SK.CMS.AES128 |  |

* + 1. **⌫**
    2. **⌦ Card-G2-A\_3447 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-K\_ObjSys\_155 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 56: Tab\_gSMC-K\_ObjSys\_155 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-K bezüglich der Zertifikate zu erlauben.
    2. **⌦ Card-G2-A\_3448 K\_Initialisierung: Initialisierte Attribute von MF / SK.CUP.AES256**
* SK.CUP.AES256 MUSS die in Tab\_gSMC-K\_ObjSys\_156 dargestellten Initialisierten Attribute besitzen.

Tabelle 57: Tab\_gSMC-K\_ObjSys\_156 Initialisierte Attribute von MF / SK.CUP.AES256

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | Symmetrisches Authentisierungsobjekt |  |
| *keyType* | AES-256 |  |
| *keyIdentifier* | ’04’ = 4 |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *encKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 256 Bit | wird personalisiert |
| *macKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 256 Bit | wird personalisiert |
| *numberScenario* | 0 |  |
| *algorithmIdentifier* | aesSessionkey4SM, siehe [gemSpec\_COS] |  |
| *accessRulesSessionkeys* | irrelevant |  |
| Zugriffsregeln | | |
| *accessRules* | identisch zu SK.CMS.AES128 |  |

* + 1. **⌫**
    2. **⌦ Card-G2-A\_3449 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-K\_ObjSys\_157 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 58: Tab\_gSMC-K\_ObjSys\_157 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.AK

* + 1. Die Anwendung DF.AK enthält kryptographische Objekte des Anwendungskonnektors.
    2. Der in dieser Anwendung enthaltene Schlüssel PrK.AK.AUT.R2048 unterstützt den Aufbau eines TLS-Kanals zwischen dem Anwendungskonnektor und dem Primärsystem. Daneben enthält die Anwendung das Zertifikat EF.C.AK.AUT.R2048, das den zugehörigen öffentlichen Schlüssel PuK.AK.AUT.R2048 enthält. Es wird als nicht erforderlich angesehen, dass die Anwendung auch Zertifikate höherer Ebenen enthält.
    3. Mit dem Schlüssel PrK.AK.CA\_PS.R2048 können X.509-Zertifikate für die Authentisierung von Clientsystemen signiert werden.
    4. Für die genannten Schlüssel sind die Nachfolger PrK.AK.AUT2.R2048 und PrK.AK.AUT.XXXX bzw. PrK.AK.CA\_PS2.R2048 und PrK.AK.CA\_PS.XXXX in der Anwendung enthalten, mit jeweils XXXX ∈ {R3072, E256, E384}. Als Nachfolger für EF.C.AK.AUT.R2048 dient die Datei EF.C.AK.AUT2.XXXX.
    5. **⌦ Card-G2-A\_2592 K\_Initialisierung: Initialisierte Attribute von MF / DF.AK**
* Das Objekt DF.AK MUSS die in Tab\_gSMC-K\_ObjSys\_032 dargestellten Werte besitzen.

Tabelle 59: Tab\_gSMC-K\_ObjSys\_032 Initialisierte Attribute von MF / DF.AK

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | Ordner |  |
| *applicationIdentifier* | ‘D276 0001 4402’ |  |
| *fileIdentifier* | herstellerspezifisch |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *shareable* | True |  |
| Zugriffsregel für logischen LCS „Operational state (activated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Get Random | ALWAYS |  |
| Load Application | PWD(PIN.Pers) |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (63) |
| Zugriffsregel für logischen LCS „Termination state“ | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (3) |

* + 1. **⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem Ordnerobjekt arbeiten, sind:   
   Activate, Deactivate, Delete, Fingerprint, Get Random, 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.5.4



Abbildung 2: Abb\_gSMC-K\_ObjSys\_002 Dateistruktur der Anwendung DF.AK

### MF /DF.AK/ EF.C.AK.AUT.R2048

* + 1. Diese Zertifikatsdatei ist angelegt, um ein Zertifikat mit dem öffentlichen Schlüssel PuK.AK.AUT.2048 zu PrK.AK.AUT.R2048 (siehe Kapitel 5.4.2) aufzunehmen.
* **⌦ Card-G2-A\_2595 K\_Initialisierung: Initialisierte Attribute von MF / DF.AK / EF.C.AK.AUT.R2048**
* Das Objekt EF.C.AK.AUT.R2048 MUSS die in Tab\_gSMC-K\_ObjSys\_034 dargestellten Werte besitzen.

Tabelle 60: Tab\_gSMC-K\_ObjSys\_034 Initialisierte Attribute von MF / DF.AK / EF.C.AK.AUT.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ‘C5 03’ |  |
| *shortFileIdentifier* | ’03’ = 3 |  |
| *numberOfOctet* | ‘08 02’ Oktett = 2.050 |  |
| *positionLogicalEndOfFile* | WildCard | 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 (65) |
| Read Binary | ALWAYS |  |
| Set Logical EOF  Write Binary | AUT\_CMS OR AUT\_CUP | siehe Hinweis (65) |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (63) |
| Zugriffsregel für logischen LCS „Termination state“ | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (63) |

* + 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 5.10.

* **⌦ Card-G2-A\_3450 K\_Personalisierung: Personalisierte Attribute von MF / DF.AK / EF.C.AK.AUT.R2048**
* Bei der Personalisierung von EF.C.AK.AUT.R2048 MÜSSEN die in Tab\_gSMC-K\_ObjSys\_158 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 61: Tab\_gSMC-K\_ObjSys\_158 Attribute von MF / DF.AK / EF.C.AK.AUT.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| *positionLogicalEndOfFile* | Zahl der tatsächlich belegten Oktette |  |
| *body* | C.AK.AUT.R2048 gemäß [gemSpec\_PKI] passend zu dem privaten Schlüssel in PrK.AK.AUT.R2048 |  |

* + 1. **⌫**

### MF / DF.AK / PrK.AK.AUT.R2048

* + 1. Dieser Schlüssel ermöglicht den Aufbau eines TLS-Kanals vom Anwendungskonnektor zum Primärsystem. Der öffentliche Teil zu diesem privaten Schlüssel ist in EF.C.AK.AUT.R2048 enthalten (siehe Kapitel 5.4.1).
    2. Aus Sicht des Primärsystems handelt der Anwendungskonnektor beim Aufbau der TLS-Verbindung als Server. Gemäß [TLS#8.1.1] wird dabei für bestimmte CipherSuites während der Serverauthentisierung eine Entschlüsselung nach [PKCS#1v2.1] Kapitel 7.2.2 durchgeführt
    3. **⌦ Card-G2-A\_2599 K\_Initialisierung: Initialisierte Attribute von MF / DF.AK / PrK.AK.AUT.R2048**
* Das Objekt PrK.AK.AUT.R2048 MUSS die in Tab\_gSMC-K\_ObjSys\_036 dargestellten Werte besitzen.

Tabelle 62: Tab\_gSMC-K\_ObjSys\_036 Initialisierte Attribute von MF / DF.AK / PrK.AK.AUT.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates Schlüsselobjekt RSA 2048 |  |
| *keyIdentifier* | ‘03’ = 3 |  |
| privateKey | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Moduluslänge 2048 Bit | wird personalisiert |
| *keyAvailable* | WildCard |  |
| *listAlgorithmIdentifier* | rsaDecipherOaep,  rsaDecipherPKCS1\_V1\_5  signPKCS1\_V1\_5,  signPSS | siehe  Hinweis (69)  Hinweis (70) |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
|  | | |
| Zugriffsart |  | 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 (68) |
| Generate Asymmetric Key Pair  P1=‘81’ | ALWAYS |  |
| PSO CompDigSig | PWD(PIN.AK) |  |
| PSO Decipher | PWD(PIN.AK) |  |
| Delete | PWD(PIN.AK) |  |
| 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. Die Zugriffsbedingung wird in Abstimmung mit den Konnektorherstellern noch festgelegt
3. Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.10
4. Wird im Rahmen von Serverauthentisierung für RSA-Ciphersuites verwendet.
5. Wird im Rahmen von Client- und Serverauthentisierung von DH-Ciphersuites verwendet.
   * 1. **⌦ Card-G2-A\_3406 K\_Personalisierung: Personalisierte Attribute von MF / DF.AK / PrK.AK.AUT.R2048**

* Bei der Personalisierung von PrK.AK.AUT.R2048 MÜSSEN die in Tab\_gSMC-K\_ObjSys\_113 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 63: Tab\_gSMC-K\_ObjSys\_113 Attribute von MF / DF.AK / PrK.AK.AUT.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| *privateKey* | Moduluslänge 2048 Bit |  |
| *keyAvailable* | True |  |

* + 1. **⌫**

### MF /DF.AK/ EF.C.AK.AUT2.XXXX

* + 1. Diese Zertifikatsdatei ist angelegt, um ein Zertifikat mit dem öffentlichen Schlüssel PuK.AK.AUT.XXXX zu PrK.AK.AUT.XXXX (XXXX aus der Menge {R2048, R3072, E256, E384}) nach Ablauf der Nutzungszeit des Schlüssels PrK.AK.AUT.R2048 aufzunehmen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.
* **⌦ Card-G2-A\_3451 K\_Initialisierung: Initialisierte Attribute von MF / DF.AK / EF.C.AK.AUT2.XXXX**
* Das Objekt EF.C.AK.AUT2.XXXX MUSS bei Ausgabe der Karte mit den in Tab\_gSMC-K\_ObjSys\_159 gezeigten Eigenschaften angelegt werden.

Tabelle 64: Tab\_gSMC-K\_ObjSys\_159 Initialisierte Attribute von MF / DF.AK / EF.C.AK.AUT2.XXXX

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ‘C5 04’ |  |
| *shortFileIdentifier* | ’04’ = 4 |  |
| *numberOfOctet* | ‘08 02’ Oktett = 2.050 |  |
| *positionLogicalEndOfFile* | ’0’ |  |
| *flagTransactionMode* | True |  |
| *flagChecksum* | False |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *shareable* | True |  |
| *body* | kein Inhalt | wird später nachgeladen |
| Zugriffsregel für logischen LCS „Operational state (activated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Delete | AUT\_CMS OR AUT\_CUP | siehe Hinweis (72) |
| Read Binary | ALWAYS |  |
| Set Logical EOF  Write Binary | AUT\_CMS OR AUT\_CUP | siehe Hinweis (72) |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (63) |
| Zugriffsregel für logischen LCS „Termination state“ | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (63) |

* + 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 5.10

### MF / DF.AK / PrK.AK.AUT2.R2048

* + 1. Dieser Schlüssel ermöglicht ebenfalls den Aufbau eines TLS-Kanals vom Anwendungskonnektor zum Primärsystem und stellt eine der Möglichkeiten dar, den Schlüssel PrK.AK.AUT.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.
* **⌦ Card-G2-A\_2597 K\_externe Welt: Erstellung des zu PrK.AK.AUT2.R2048 gehörenden Zertifikats**
* Nach Auslesen des öffentlichen Schlüssels mit Generate Asymmetric Key Pair MUSS das dazugehörende Zertifikat erstellt und in EF.C.AK.AUT2.XXXX gespeichert werden.
  + 1. **⌫**
    2. **⌦ Card-G2-A\_3452 K\_Initialisierung: Initialisierte Attribute von MF / DF.AK / PrK.AK.AUT2.R2048**
* Das Objekt PrK.AK.AUT2.R2048 MUSS die in Tab\_gSMC-K\_ObjSys\_187 dargestellten Werte besitzen.

Tabelle 65: Tab\_gSMC-K\_ObjSys\_187 Initialisierte Attribute von MF / DF.AK / PrK.AK.AUT2.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates Schlüsselobjekt RSA 2048 |  |
| *keyIdentifier* | ‘04’ = 4 |  |
| privateKey | Speicherplatz hinreichend für einen Schlüssel mit Moduluslänge 2048 Bit | wird später mit Generate Asymmetric Key Pair erzeugt |
| *keyAvailable* | False |  |
| *listAlgorithmIdentifier* | rsaDecipherOaep,  rsaDecipherPKCS1\_V1\_5  signPKCS1\_V1\_5,  signPSS | siehe  Hinweis (69)  Hinweis (70) |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregeln | | |
| *accessRules* | identisch zu PrK.AK.AUT.R2048 |  |

* + 1. **⌫**

### MF / DF.AK / PrK.AK.AUT.R3072

* + 1. Dieser Schlüssel ermöglicht ebenfalls den Aufbau eines TLS-Kanals vom Anwendungskonnektor zum Primärsystem und stellt eine der Möglichkeiten dar, den Schlüssel PrK.AK.AUT.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.
    2. **⌦ Card-G2-A\_3253 K\_externe Welt: Erstellung der zu PrK.AK.AUT.R3072 gehörenden Zertifikate**
* Nach Auslesen des öffentlichen Schlüssels mit Generate Asymmetric Key Pair MUSS das dazugehörende Zertifikat erstellt und in EF.C.AK.AUT2.XXXX gespeichert werden.
  + 1. **⌫**
    2. **⌦ Card-G2-A\_3254 K\_Initialisierung: Initialisierte Attribute von MF / DF.AK / PrK.AK.AUT.R3072**
* Das Objekt PrK.AK.AUT.R3072 MUSS die in Tab\_gSMC-K\_ObjSys\_160 dargestellten Werte besitzen.

Tabelle 66: Tab\_gSMC-K\_ObjSys\_160 Initialisierte Attribute von MF / DF.AK / PrK.AK.AUT.R3072

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates RSA Schlüsselobjekt R3072 |  |
| *keyIdentifier* | 05’ = 5 |  |
| privateKey | Speicherplatz hinreichend für einen Schlüssel mit Moduluslänge 3072 Bit | wird später mit Generate Asymmetric Key Pair erzeugt |
| *keyAvailable* | False |  |
| *listAlgorithmIdentifier* | rsaDecipherOaep,  rsaDecipherPKCS1\_V1\_5  signPKCS1\_V1\_5,  signPSS | siehe  Hinweis (69)  Hinweis (70) |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregeln | | |
| *accessRules* | identisch zu PrK.AK.AUT.R2048 |  |

* + 1. **⌫**

### MF / DF.AK / PrK.AK.AUT.E256

* + 1. Dieser Schlüssel ermöglicht ebenfalls den Aufbau eines TLS-Kanals vom Anwendungskonnektor zum Primärsystem und stellt eine der Möglichkeiten dar, den Schlüssel PrK.AK.AUT.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.
    2. **⌦ Card-G2-A\_3255 K\_externe Welt: Erstellung der zu PrK.AK.AUT.E256 gehörenden Zertifikate**
* Nach Auslesen des öffentlichen Schlüssels mit Generate Asymmetric Key Pair MUSS das dazugehörende Zertifikat erstellt und in EF.C.AK.AUT2.XXXX gespeichert werden.
  + 1. **⌫**
    2. **⌦ Card-G2-A\_3256 K\_Initialisierung: Initialisierte Attribute von MF / DF.AK / PrK.AK.AUT.E256**
* Das Objekt PrK.AK.AUT.E256 MUSS die in Tab\_gSMC-K\_ObjSys\_161 dargestellten Werte besitzen.

Tabelle 67: Tab\_gSMC-K\_ObjSys\_161 Initialisierte Attribute von MF / DF.AK / PrK.AK.AUT.E256

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates ELC Schlüsselobjekt E256 |  |
| *keyIdentifier* | ‘07’ = 7 |  |
| *privateElcKey* | domainparameter = brainpoolP256r1 | wird später mit Generate Asymmetric Key Pair erzeugt |
| *privateElcKey* | keyData = AttributNotSet |  |
| *keyAvailable* | False |  |
| *listAlgorithmIdentifier* | elcSharedSecretCalculation, signECDSA | siehe  Hinweis (69)  Hinweis (70) |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregeln | | |
| *accessRules* | identisch zu PrK.AK.AUT.R2048 |  |

* + 1. **⌫**

### MF / DF.AK / PrK.AK.AUT.E384

* + 1. Dieser Schlüssel ermöglicht ebenfalls den Aufbau eines TLS-Kanals vom Anwendungskonnektor zum Primärsystem und stellt eine der Möglichkeiten dar, den Schlüssel PrK.AK.AUT.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.
    2. **⌦ Card-G2-A\_3257 K\_externe Welt: Erstellung der zu PrK.AK.AUT.E384 gehörenden Zertifikate**
* Nach Auslesen des öffentlichen Schlüssels mit Generate Asymmetric Key Pair MUSS das dazugehörende Zertifikat erstellt und in EF.C.AK.AUT2.XXXX gespeichert werden.
  + 1. **⌫**
    2. **⌦ Card-G2-A\_3258 K\_Initialisierung: Initialisierte Attribute von MF / DF.AK / PrK.AK.AUT.E384**
* Das Objekt PrK.AK.AUT.E384 MUSS die in Tab\_gSMC-K\_ObjSys\_162 dargestellten Werte besitzen.

Tabelle 68: Tab\_gSMC-K\_ObjSys\_162 Initialisierte Attribute von MF / DF.AK / PrK.AK.AUT.E384

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates ELC Schlüsselobjekt E384 |  |
| *keyIdentifier* | ‘06’ = 6 |  |
| *privateElcKey* | domainparameter = brainpoolP384r1 | wird später mit Generate Asymmetric Key Pair erzeugt |
| *privateElcKey* | keyData = AttributNotSet |  |
| *keyAvailable* | False |  |
| *listAlgorithmIdentifier* | elcSharedSecretCalculation, signECDSA | siehe  Hinweis (69)  Hinweis (70) |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregeln | | |
| *accessRules* | identisch zu PrK.AK.AUT.R2048 |  |

* + 1. **⌫**

### MF / DF.AK / PrK.AK.CA\_PS.R2048

* + 1. Dieser private Schlüssel für die Kryptographie mit RSA dient herstellerspezifischen Zwecken; mit diesem Schlüssel können X.509-Zertifikate für die Authentisierung von Clientsystemen signiert werden. Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos Generate Asymmetric Key Pair (siehe [gemSpec\_COS#14.9.3.4]) auslesen.
    2. **⌦ Card-G2-A\_2600 K\_Initialisierung: Initialisierte Attribute von MF / DF.AK / PrK.AK.CA\_PS.R2048**
* Das Objekt PrK.AK.CA\_PS.R2048 MUSS die in Tab\_gSMC-K\_ObjSys\_037 dargestellten Werte besitzen.

Tabelle 69: Tab\_gSMC-K\_ObjSys\_037 Initialisierte Attribute von MF / DF.AK / PrK.AK.CA\_PS.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates RSA Schlüsselobjekt |  |
| *keyIdentifier* | ‘08’ = 8 |  |
| *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]  {sign9796\_2\_DS2, signPKCS1\_V1\_5, signPSS} |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregel für logischen LCS „Operational state (activated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Generate Asymmetric Key Pair  P1=‘84’ oder P1=’80’ | PWD(PIN.AK) | Siehe Hinweis (74) |
| Generate Asymmetric Key Pair  P1=‘81’ | ALWAYS |  |
| PSO CompDigSig | PWD(PIN.AK) |  |
| Terminate | PWD(PIN.AK) |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (63) |
| 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. Die Zugriffsbedingung wird in Abstimmung mit den Konnektorherstellern noch festgelegt
   * 1. **⌦ Card-G2-A\_3407 K\_Personalisierung: Personalisierte Attribute von MF / DF.AK / PrK.AK.CA\_PS.R2048**

* Bei der Personalisierung von PrK.AK.CA\_PS.R2048 MÜSSEN die in Tab\_gSMC-K\_ObjSys\_114 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 70: Tab\_gSMC-K\_ObjSys\_114 Attribute von MF / DF.AK / PrK.AK.CA\_PS.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| *privateKey* | Moduluslänge 2048 Bit |  |
| *keyAvailable* | True |  |

* + 1. **⌫**

### MF / DF.AK / PrK.AK.CA\_PS2.R2048

* + 1. Dieser private Schlüssel für die Kryptographie mit RSA dient ebenfalls herstellerspezifischen Zwecken; mit diesem Schlüssel können X.509-Zertifikate für die Authentisierung von Clientsystemen signiert werden. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.AK.AUT.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.. Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos Generate Asymmetric Key Pair (siehe [gemSpec\_COS#14.9.3.4]) auslesen.
    2. **⌦ Card-G2-A\_3408 K\_Initialisierung: Initialisierte Attribute von MF / DF.AK / PrK.AK.CA\_PS2.R2048**
* Das Objekt PrK.AK.CA\_PS2.R2048 MUSS die in Tab\_gSMC-K\_ObjSys\_180 dargestellten Werte besitzen.

Tabelle 71: Tab\_gSMC-K\_ObjSys\_180 Initialisierte Attribute von MF / DF.AK / PrK.AK.CA\_PS2.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates RSA Schlüsselobjekt |  |
| *keyIdentifier* | ‘09’ = 9 |  |
| *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]  {sign9796\_2\_DS2, signPKCS1\_V1\_5, signPSS} |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregeln | | |
| *accessRules* | identisch zu PrK.AK.CA\_PS.R2048 |  |

* + 1. **⌫**

### MF / DF.AK / PrK.AK.CA\_PS.R3072

* + 1. Dieser private Schlüssel für die Kryptographie mit RSA dient ebenfalls herstellerspezifischen Zwecken; mit diesem Schlüssel können X.509-Zertifikate für die Authentisierung von Clientsystemen signiert werden. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.AK.AUT.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen. Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos Generate Asymmetric Key Pair (siehe [gemSpec\_COS#14.9.3.4]) auslesen.
    2. **⌦ Card-G2-A\_2601 K\_Initialisierung: Initialisierte Attribute von MF / DF.AK / PrK.AK.CA\_PS.R3072**
* Das Objekt PrK.AK.CA\_PS.R3072 MUSS die in Tab\_gSMC-K\_ObjSys\_038 dargestellten Werte besitzen.

Tabelle 72: Tab\_gSMC-K\_ObjSys\_038 Initialisierte Attribute von MF / DF.AK / PrK.AK.CA\_PS.R3072

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates RSA Schlüsselobjekt |  |
| *keyIdentifier* | ‘0D’ = 13 |  |
| 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]  {sign9796\_2\_DS2, signPKCS1\_V1\_5, signPSS} |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregeln | | |
| *accessRules* | identisch zu PrK.AK.CA\_PS.R2048 |  |

* + 1. **⌫**

### MF / DF.AK / PrK.AK.CA\_PS.E256

* + 1. Dieser private Schlüssel für die Kryptographie mit ELC dient ebenfalls herstellerspezifischen Zwecken; mit diesem Schlüssel können X.509-Zertifikate für die Authentisierung von Clientsystemen signiert werden. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.AK.AUT.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.. Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos Generate Asymmetric Key Pair (siehe [gemSpec\_COS#14.9.3.4]) auslesen.
    2. **⌦ Card-G2-A\_3409 K\_Initialisierung: Initialisierte Attribute von MF / DF.AK / PrK.AK.CA\_PS.E256**
* Das Objekt PrK.AK.CA\_PS.E256 MUSS die in Tab\_gSMC-K\_ObjSys\_181 dargestellten Werte besitzen.

Tabelle 73: Tab\_gSMC-K\_ObjSys\_181 Initialisierte Attribute von MF / DF.AK / PrK.AK.CA\_PS.E256

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates ELC Schlüsselobjekt |  |
| *keyIdentifier* | ‘10’ = 16 |  |
| *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]  {signECDSA } |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregeln | | |
| *accessRules* | identisch zu PrK.AK.CA\_PS.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

### MF / DF.AK / PrK.AK.CA\_PS.E384

* + 1. Dieser private Schlüssel für die Kryptographie mit ELC dient ebenfalls herstellerspezifischen Zwecken; mit diesem Schlüssel können X.509-Zertifikate für die Authentisierung von Clientsystemen signiert werden. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.AK.AUT.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen. Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos Generate Asymmetric Key Pair (siehe [gemSpec\_COS#14.9.3.4]) auslesen.
    2. **⌦ Card-G2-A\_2602 K\_Initialisierung: Initialisierte Attribute von MF / DF.AK / PrK.AK.CA\_PS.E384**
* Das Objekt PrK.AK.CA\_PS.E384 MUSS die in Tab\_gSMC-K\_ObjSys\_039 dargestellten Werte besitzen.

Tabelle 74: Tab\_gSMC-K\_ObjSys\_039 Initialisierte Attribute von MF / DF.AK / PrK.AK.CA\_PS.E384

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates ELC Schlüsselobjekt |  |
| *keyIdentifier* | ‘11’ = 17 |  |
| *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]  {signECDSA } |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregeln | | |
| *accessRules* | identisch zu PrK.AK.CA\_PS.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

## MF / DF.NK

* + 1. Die Anwendung DF.NK enthält kryptographische Objekte des Netzkonnektors.
    2. Der in dieser Anwendung enthaltene Schlüssel PrK.NK.VPN (in der jeweils aktuellen Ausprägung) unterstützt den Aufbau einer VPN-Verbindung zum VPN-Konzentrator.
    3. Diese Anwendung enthält neben den vorgenannten privaten Schlüsseln pro privatem Schlüssel ein Zertifikat mit dem öffentlichen Schlüssel zum jeweiligen privaten Schlüssel. Es wird als nicht erforderlich angesehen, dass die Anwendung auch Zertifikate höherer Ebenen enthält.
    4. **⌦ Card-G2-A\_2605 K\_Initialisierung: Initialisierte Attribute von MF / DF.NK**
* Das Objekt DF.NK MUSS die in Tab\_gSMC-K\_ObjSys\_040 dargestellten Werte besitzen.



Tabelle 75: Tab\_gSMC-K\_ObjSys\_040 Initialisierte Attribute von MF / DF.NK

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute | Wert | | Bemerkung |
| Objekttyp | Ordner | |  |
| *applicationIdentifier* | ‘D276 0001 4403’ | |  |
| *fileIdentifier* | ’AA00’ | |  |
| *lifeCycleStatus* | „Operational state (activated)“ | |  |
| *shareable* | True | |  |
| Zugriffsregel für logischen LCS „Operational state (activated)” | | | |
| Zugriffsart | Zugriffsbedingung | | Bemerkung |
| Get Random | ALWAYS |  | |
| Load Application | PWD(PIN.Pers) |  | |
| andere | NEVER | |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | | |
| Zugriffsart | Zugriffsbedingung | | Bemerkung |
| alle | herstellerspezifisch | | siehe Hinweis (78) |
| Zugriffsregel für logischen LCS „Termination state“ | | | |
| Zugriffsart | Zugriffsbedingung | | Bemerkung |
| alle | herstellerspezifisch | | siehe Hinweis (78) |

* + 1. **⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem Ordnerobjekt arbeiten, sind:   
   Activate, Deactivate, Delete, Fingerprint, Get Random, 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 5.5 im Allgemeinen irrelevant.



Abbildung 3: Abb\_gSMC-K\_ObjSys\_003 Dateistruktur der Anwendung DF.NK

### MF / DF.NK / EF.ActKey

* + 1. Diese Datei ist in der Lage; Informationen über den aktuell zu verwendenden Schlüssel zu speichern. Inhalt und Verwendung dieser Datei sind herstellerspezifisch.
    2. **⌦ Card-G2-A\_2606 K\_Initialisierung: Initialisierte Attribute von MF / DF.NK / EF.ActKey**
* Das Objekt EF.ActKey MUSS die in Tab\_gSMC-K\_ObjSys\_041 dargestellten Werte besitzen.

Tabelle 76: Tab\_gSMC-K\_ObjSys\_041 Initialisierte Attribute von MF / DF.NK / EF.ActKey

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ‘FE 05’ |  |
| *shortFileIdentifier* | – |  |
| *numberOfOctet* | ‘000B’ Oktett = 11 Oktett |  |
| *positionLogicalEndOfFile* | ’0’ |  |
| *flagTransactionMode* | True |  |
| *flagChecksum* | True |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *shareable* | True |  |
| *body* | kein Inhalt |  |
| Zugriffsregel für logischen LCS „Operational state (activated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Read Binary | PWD(PIN.NK) | siehe Hinweis (80) |
| Erase Binary  Set Logical EOF  Update Binary  Write Binary | PWD(PIN.NK) | siehe Hinweis (80) |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (78) |
| Zugriffsregel für logischen LCS „Termination state“ | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (78) |

* + 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 5.10

### MF / DF.NK / EF.CardInfo

* + 1. Diese Datei ist in der Lage Kartenparameter des Netzkonnektors zu speichern. Inhalt und Verwendung dieser Datei ist herstellerspezifisch.
    2. **⌦ Card-G2-A\_2607 K\_Initialisierung: Initialisierte Attribute von MF / DF.NK / EF.CardInfo**
* Das Objekt EF.CardInfo MUSS die in Tab\_gSMC-K\_ObjSys\_042 dargestellten Werte besitzen.

Tabelle 77: Tab\_gSMC-K\_ObjSys\_042 Initialisierte Attribute von MF / DF.NK / EF.CardInfo

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ‘A2 00’ |  |
| *shortFileIdentifier* | – |  |
| *numberOfOctet* | ‘000A’ Oktett = 10 Oktett |  |
| *positionLogicalEndOfFile* | ’0’ |  |
| *flagTransactionMode* | True |  |
| *flagChecksum* | True |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *shareable* | True |  |
| *body* | kein Inhalt |  |
| Zugriffsregel für logischen LCS „Operational state (activated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Read Binary | ALWAYS |  |
| Erase Binary  Set Logical EOF  Update Binary  Write Binary | PWD(PIN.NK) |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (78) |
| Zugriffsregel für logischen LCS „Termination state“ | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (78) |

* + 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.NK / EF.CFSMACKey

* + 1. Diese Datei ist in der Lage Informationen über das Dateisystem des Netzkonnektors zu speichern. Inhalt und Verwendung dieser Datei ist herstellerspezifisch.
    2. **⌦ Card-G2-A\_2608 K\_Initialisierung: Initialisierte Attribute von MF / DF.NK / EF.CFSMACKey**
* Das Objekt EF.CFSMACKey MUSS die in Tab\_gSMC-K\_ObjSys\_043 dargestellten Werte besitzen.

Tabelle 78: Tab\_gSMC-K\_ObjSys\_043 Initialisierte Attribute von MF / DF.NK / EF.CFSMACKey

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ‘A1 07’ |  |
| *shortFileIdentifier* | – |  |
| *numberOfOctet* | ‘0034’ Oktett = 52 Oktett |  |
| *positionLogicalEndOfFile* | ’0’ |  |
| *flagTransactionMode* | True |  |
| *flagChecksum* | True |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *shareable* | True |  |
| *body* | kein Inhalt |  |
| Zugriffsregel für logischen LCS „Operational state (activated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Read Binary | PWD(PIN.NK) |  |
| Erase Binary  Set Logical EOF  Update Binary  Write Binary | PWD(PIN.NK) |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (78) |
| Zugriffsregel für logischen LCS „Termination state“ | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (78) |

* + 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.NK / EF.ConfigUser

* + 1. Diese Datei ist in der Lage Konfigurationsinformationen zu speichern. Inhalt und Verwendung dieser Datei ist herstellerspezifisch.
    2. **⌦ Card-G2-A\_2609 K\_Initialisierung: Initialisierte Attribute von** **MF / DF.NK / EF.ConfigUser**
* Das Objekt EF.ConfigUser MUSS die in Tab\_gSMC-K\_ObjSys\_044 dargestellten Werte besitzen.

Tabelle 79: Tab\_gSMC-K\_ObjSys\_044 Initialisierte Attribute von MF / DF.NK / EF.ConfigUser

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ‘A1 00’ |  |
| *shortFileIdentifier* | – |  |
| *numberOfOctet* | ‘00C8’ Oktett = 200 Oktett |  |
| *positionLogicalEndOfFile* | ’0’ |  |
| *flagTransactionMode* | True |  |
| *flagChecksum* | True |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *shareable* | True |  |
| *body* | kein Inhalt |  |
| Zugriffsregel für logischen LCS „Operational state (activated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Read Binary | PWD(PIN.NK) |  |
| Erase Binary  Set Logical EOF  Update Binary  Write Binary | PWD(PIN.NK) |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (78) |
| Zugriffsregel für logischen LCS „Termination state“ | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (78) |

* + 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.NK/ EF.C.NK.VPN.R2048

* + 1. Diese Zertifikatsdatei enthält das Zertifikat mit dem öffentlichen Schlüssel zu PrK.NK.VPN.R2048 (siehe Kapitel 5.5.6).
    2. **⌦ Card-G2-A\_2612 K\_Initialisierung: Initialisierte Attribute von MF / DF.NK / EF.C.NK.VPN.R2048**
* Das Objekt EF.C.NK.VPN.R2048 MUSS die in Tab\_gSMC-K\_ObjSys\_046 dargestellten Werte besitzen.

Tabelle 80: Tab\_gSMC-K\_ObjSys\_046 Initialisierte Attribute von MF / DF.NK / EF.C.NK.VPN.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ‘C5 05’ |  |
| *shortFileIdentifier* | ’05’ = 5 |  |
| *numberOfOctet* | ‘08 02’ Oktett = 2.050 Oktett |  |
| *positionLogicalEndOfFile* | WildCard | 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 (88) |
| Read Binary | PWD(PIN.NK) |  |
| Set Logical EOF  Write Binary | AUT\_CMS OR AUT\_CUP | siehe Hinweis (88) |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (78) |
| Zugriffsregel für logischen LCS „Termination state“ | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (78) |

* + 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- bzw. CUP-Schlüssels ausführbar, siehe Kapitel 5.10.
   * 1. **⌦ Card-G2-A\_3410 K\_Personalisierung: Personalisierte Attribute von MF / DF.NK / EF.C.NK.VPN.R2048**

* Die Objekte EF.C.NK.VPN.R2048 MÜSSEN gemäß der in Tab\_gSMC-K\_ObjSys\_121 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 81: Tab\_gSMC-K\_ObjSys\_121 Attribute von MF / DF.NK / EF.C.NK.VPN.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| *positionLogicalEndOfFile* | Zahl der tatsächlich belegten Oktette |  |
| *body* | C.NK.VPN.R2048 gemäß [gemSpec\_PKI] passend zu dem privaten Schlüssel in PrK.NK.VPN.R2048 |  |

* + 1. **⌫**

### MF / DF.NK / PrK.NK.VPN.R2048

* + 1. Dieser private Schlüssel für die Kryptographie mit RSA dient der Verbindung des Netzkonnektors mit dem VPN-Gateway. Der zugehörende öffentliche Schlüssel PuK.NK.VPN.R2048 ist im Zertifikat EF.C.NK.VPN.R2048 enthalten.
    2. **⌦ Card-G2-A\_3259 K\_Initialisierung: Initialisierte Attribute von MF / DF.NK / PrK.NK.VPN.R2048**
* Das Objekt PrK.NK.VPN.R2048 MUSS die in Tab\_gSMC-K\_ObjSys\_188 dargestellten Werte besitzen.

Tabelle 82: Tab\_gSMC-K\_ObjSys\_188 Initialisierte Attribute von MF / DF.NK / PrK.NK.VPN.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates Schlüsselobjekt, RSA 2048 |  |
| *keyIdentifier* | ‘05’ = 5 |  |
| *privateKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Moduluslänge 2048 Bit | wird personalisiert |
| *keyAvailable* | WildCard |  |
| *listAlgorithmIdentifier* | rsaDecipherPKCS1\_V1\_5, signPKCS1\_V1\_5, rsaDecipherOaep signPSS |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregel für logischen LCS „Operational state (activated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Deactivate | AUT\_CMS OR AUT\_CUP | Siehe Hinweis (90) |
| Activate | ALWAYS | herstellerspezifisch ist eine der beiden Varianten erlaubt |
| 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 | Siehe Hinweis (90) |
| PSO CompDigSig | PWD(PIN.NK) |  |
| PSO Decipher | PWD(PIN.NK) |  |
| Delete | PWD(PIN.NK)  OR AUT\_CMS OR AUT\_CUP |  |
| 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. Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.10
   * 1. **⌦ Card-G2-A\_3411 K\_Personalisierung: Personalisierte Attribute von MF / DF.NK / PrK.NK.VPN.R2048**

* Bei der Personalisierung von PrK.NK.VPN.R2048 MÜSSEN die in Tab\_gSMC-K\_ObjSys\_163 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 83: Tab\_gSMC-K\_ObjSys\_163 Attribute von MF / DF.NK / PrK.NK.VPN.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| *privateKey* | Moduluslänge 2048 Bit |  |
| *keyAvailable* | True |  |

* + 1. **⌫**

### MF /DF.NK/ EF.C.NK.VPN2.XXXX

* + 1. Diese Zertifikatsdatei ist angelegt, um ein Zertifikat mit dem öffentlichen Schlüssel PuK.NK.VPN.XXXX zu PrK.NK.VPN.XXXX (XXXX aus der Menge {R2048, R3072, E256, E384}) nach Ablauf der Nutzungszeit des Schlüssels PrK.AK.AUT.R2048 aufzunehmen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.
    2. **⌦ Card-G2-A\_3260 K\_Initialisierung: Initialisierte Attribute von MF / DF.NK / EF.C.NK.VPN2.XXXX**
* Das Objekt EF.C.NK.VPN2.XXXX MUSS bei Ausgabe der Karte mit den in Tab\_gSMC-K\_ObjSys\_189 dargestellten Werte angelegt werden.

Tabelle 84: Tab\_gSMC-K\_ObjSys\_189 Initialisierte Attribute von MF / DF.NK / EF.C.NK.VPN2.XXXX

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ‘C5 06’ |  |
| *shortFileIdentifier* | ’06’ = 6 |  |
| *numberOfOctet* | ‘08 02’ Oktett = 2.050 Oktett |  |
| *positionLogicalEndOfFile* | ’0’ |  |
| *flagTransactionMode* | True |  |
| *flagChecksum* | False |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *shareable* | True |  |
| *body* | kein Inhalt | wird später nachgeladen |
| Zugriffsregel für logischen LCS „Operational state (activated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Delete | AUT\_CMS OR AUT\_CUP | siehe Hinweis (92) |
| Read Binary | PWD(PIN.NK) |  |
| Set Logical EOF  Write Binary | AUT\_CMS OR AUT\_CUP | siehe Hinweis (92) |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (78) |
| Zugriffsregel für logischen LCS „Termination state“ | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (78) |

* + 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 5.10

### MF / DF.NK / PrK.NK.VPN2.R2048

* + 1. Dieser private Schlüssel für die Kryptographie mit RSA wird ebenfalls zur Verbindung des Netzkonnektors mit dem VPN-Gateway genutzt. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.NK.VPN.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen. Der zugehörende öffentliche Schlüssel PuK.NK.VPN2.R2048 ist im Zertifikat EF.C.NK.VPN2.XXXX enthalten.
    2. **⌦ Card-G2-A\_3412 K\_Initialisierung: Initialisierte Attribute von MF / DF.NK / PrK.NK.VPN2.R2048**
* Das Objekt PrK.NK.VPN2.R2048 MUSS die in Tab\_gSMC-K\_ObjSys\_164 dargestellten Werte besitzen.

Tabelle 85: Tab\_gSMC-K\_ObjSys\_164 Initialisierte Attribute von MF / DF.NK / PrK.NK.VPN2.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates Schlüsselobjekt, RSA 2048 |  |
| *keyIdentifier* | ‘06’ = 6 |  |
| *privateKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Moduluslänge 2048 Bit | wird später mit Generate Asymmetric Key Pair erzeugt |
| *keyAvailable* | False |  |
| *listAlgorithmIdentifier* | rsaDecipherPKCS1\_V1\_5, rsaDecipherOaep signPKCS1\_V1\_5, signPSS |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregeln | | |
| *accessRules* | identisch zu PrK.NK.VPN.R2048 |  |

* + 1. **⌫**

### MF / DF.NK / PrK.NK.VPN.R3072

* + 1. Dieser private Schlüssel für die Kryptographie mit RSA wird ebenfalls zur Verbindung des Netzkonnektors mit dem VPN-Gateway genutzt. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.NK.VPN.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen. Der zugehörende öffentliche Schlüssel PuK.NK.VPN2.R3072 ist im Zertifikat EF.C.NK.VPN2.XXXX enthalten.
    2. **⌦ Card-G2-A\_3413 K\_Initialisierung: Initialisierte Attribute von MF / DF.NK / PrK.NK.VPN.R3072**
* Das Objekt PrK.NK.VPN.R3072 MUSS die in Tab\_gSMC-K\_ObjSys\_190 dargestellten Werte besitzen.

Tabelle 86: Tab\_gSMC-K\_ObjSys\_190 Initialisierte Attribute von MF / DF.NK / PrK.NK.VPN.R3072

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates Schlüsselobjekt, RSA 3072 |  |
| *keyIdentifier* | ‘07’ = 7 |  |
| *privateKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Moduluslänge 3072 Bit | wird später mit Generate Asymmetric Key Pair erzeugt |
| *keyAvailable* | False |  |
| *listAlgorithmIdentifier* | rsaDecipherPKCS1\_V1\_5, rsaDecipherOaep signPKCS1\_V1\_5, signPSS |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregeln | | |
| *accessRules* | identisch zu PrK.NK.VPN.R2048 |  |

* + 1. **⌫**

### MF / DF.NK / PrK.NK.VPN.E256

* + 1. Dieser private Schlüssel für die Kryptographie mit elliptischen Kurven wird ebenfalls zur Verbindung des Netzkonnektors mit dem VPN-Gateway genutzt. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.NK.VPN.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen. Der zugehörende öffentliche Schlüssel PuK.NK.VPN2.E256 ist im Zertifikat EF.C.NK.VPN2.XXXX enthalten.
    2. **⌦ Card-G2-A\_3414 K\_Initialisierung: Initialisierte Attribute von MF / DF.NK / PrK.NK.VPN.E256**
* Das Objekt PrK.NK.VPN.E256 MUSS die in Tab\_gSMC-K\_ObjSys\_165 dargestellten Werte besitzen.

Tabelle 87: Tab\_gSMC-K\_ObjSys\_165 Initialisierte Attribute von MF / DF.NK / PrK.NK.VPN.E256

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates Schlüsselobjekt, ELC 256 |  |
| *keyIdentifier* | ‘0A’ = 10 |  |
| *privateElcKey* | domainparameter = brainpoolP256r1 | wird später mit Generate Asymmetric Key Pair erzeugt |
| *privateElcKey* | keyData = AttributNotSet |  |
| *keyAvailable* | False |  |
| *listAlgorithmIdentifier* | elcSharedSecretCalculation, signECDSA |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregeln | | |
| *accessRules* | identisch zu PrK.NK.VPN.R2048 |  |

* + 1. **⌫**

### MF / DF.NK / PrK.NK.VPN.E384

* + 1. Dieser private Schlüssel für die Kryptographie mit elliptischen Kurven wird ebenfalls zur Verbindung des Netzkonnektors mit dem VPN-Gateway genutzt. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.NK.VPN.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen. Der zugehörende öffentliche Schlüssel PuK.NK.VPN2.E384 ist im Zertifikat EF.C.NK.VPN2.XXXX enthalten.
    2. **⌦ Card-G2-A\_3415 K\_Initialisierung: Initialisierte Attribute von MF / DF.NK / PrK.NK.VPN.E384**
* Das Objekt PrK.NK.VPN.E384 MUSS die in Tab\_gSMC-K\_ObjSys\_166 dargestellten Werte besitzen.

Tabelle 88: Tab\_gSMC-K\_ObjSys\_166 Initialisierte Attribute von MF / DF.NK / PrK.NK.VPN.E384

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates Schlüsselobjekt, ELC 384 |  |
| *keyIdentifier* | ‘08’ = 8 |  |
| *privateElcKey* | domainparameter = brainpoolP384r1 | wird später mit Generate Asymmetric Key Pair erzeugt |
| *privateElcKey* | keyData = AttributNotSet |  |
| *keyAvailable* | False |  |
| *listAlgorithmIdentifier* | elcSharedSecretCalculation, signECDSA |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregeln | | |
| *accessRules* | identisch zu PrK.NK.VPN.R2048 |  |

* + 1. **⌫**

### MF / DF.NK / PrK.CFS.R2048

* + 1. Dieser private Schlüssel für die Kryptographie mit RSA dient herstellerspezifischen Zwecken. Er unterstützt das Signieren und das Entschlüsseln von Daten. Der zugehörige öffent­liche Schlüssel ist PuK.CFS.R2048 (siehe Kapitel 5.5.13). Er lässt sich auch mittels des Kommandos Generate Asymmetric Key Pair (siehe [gem­Spec\_COS#14.9.3.4]) auslesen.
    2. **⌦ Card-G2-A\_2617 K\_Initialisierung: Initialisierte Attribute von MF / DF.NK / PrK.CFS.R2048**
* Das Objekt PrK.CFS.R2048 MUSS die in Tab\_gSMC-K\_ObjSys\_049 dargestellten Werte besitzen.

Tabelle 89: Tab\_gSMC-K\_ObjSys\_049 Initialisierte Attribute von MF / DF.NK / PrK.CFS.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates RSA-Schlüsselobjekt |  |
| *keyIdentifier* | ‘09’ = 9 |  |
| *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]  { signPSS,  rsaDecipherOaep,  rsaDecipherPKCS1\_V1\_5  signPKCS1\_V1\_5,  } |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregel für logischen LCS „Operational state (activated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Generate Asymmetric Key Pair  P1=‘84’ oder P1=’80’ | PWD(PIN.NK) |  |
| Generate Asymmetric Key Pair  P1=‘81’ | ALWAYS |  |
| PSO CompDigSig | PWD(PIN.NK) |  |
| PSO Decipher | PWD(PIN.NK) |  |
| PSO Transcipher | PWD(PIN.NK) |  |
| Terminate | PWD(PIN.NK) |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (78) |
| 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
   * 1. **⌦ Card-G2-A\_3416 K\_Personalisierung: Personalisierte Attribute von MF / DF.NK / PrK.CFS.R2048**

* Bei der Personalisierung von PrK.CFS.R2048 MÜSSEN die in Tab\_gSMC-K\_ObjSys\_123 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 90: Tab\_gSMC-K\_ObjSys\_123 Attribute von MF / DF.NK / PrK.CFS.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| *privateKey* | Moduluslänge 2048 Bit |  |
| *keyAvailable* | True |  |

* + 1. **⌫**

### MF / DF.NK / PuK.CFS.R2048

* + 1. Dieses Objekt enthält den öffentlichen Schlüssel für die Kryptographie mit RSA zu PrK.CFS.R2048 (siehe Kapitel 5.5.12). Der öffentliche Schlüssel dient der Verschlüsselung von Daten.
    2. **⌦ Card-G2-A\_2623 K\_Initialisierung: Initialisierte Attribute von MF / DF.NK / PuK.CFS.R2048**
* Das Objekt PuK.CFS.R2048 MUSS die in Tab\_gSMC-K\_ObjSys\_055 dargestellten Werte besitzen.

Tabelle 91: Tab\_gSMC-K\_ObjSys\_055 Initialisierte Attribute von MF / DF.NK / PuK.CFS.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | öffentliches RSA Verschlüsselungsobjekt |  |
| *keyIdentifier* | '000000000000000000000019’ |  |
| *publicKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Moduluslänge 2048 Bit | wird personalisiert |
| *oid* | Id-rsaEncipherOaep |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregel für logischen LCS „Operational state (activated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| PSO Encipher | ALWAYS |  |
| Terminate | PWD(PIN.NK) | siehe Hinweis (95) |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (3) |
| Zugriffsregel für logischen LCS „Termination state” kontaktbehaftet | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | NEVER |  |

* + 1. **⌫**

1. Kommandos, die gemäß [gemSpec\_COS#8.6.4.3] mit einem öffentlichen Verschlüsselungsobjekt arbeiten sind: PSO Encipher, Terminate
2. Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kapitel 5.10.
   * 1. **⌦ Card-G2-A\_3417 K\_Personalisierung: Personalisierte Attribute von MF / DF.NK / PuK.CFS.R2048**

* Bei der Personalisierung von PuK.CFS.R2048 MÜSSEN die in Tab\_gSMC-K\_ObjSys\_130 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 92: Tab\_gSMC-K\_ObjSys\_130 Attribute von MF / DF.NK / PuK.CFS.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| *publicKey* | Moduluslänge 2048 Bit |  |

* + 1. **⌫**

### MF / DF.NK / PrK.CFS2.R2048

* + 1. Dieser private Schlüssel für die Kryptographie mit RSA dient ebenfalls herstellerspezifischen Zwecken. Er unterstützt das Signieren und das Entschlüsseln von Daten. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.CFS.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.
    2. Der zugehörige öffent­liche Schlüssel PuK.CFS2.R2048 lässt sich mittels des Kommandos Generate Asymmetric Key Pair (siehe [gem­Spec\_COS#14.9.3.4]) aus diesem Objekt auslesen.
    3. **⌦ Card-G2-A\_3418 K\_Initialisierung: Initialisierte Attribute von MF / DF.NK / PrK.CFS2.R2048**
* Das Objekt PrK.CFS2.R2048 MUSS die in Tab\_gSMC-K\_ObjSys\_182 dargestellten Werte besitzen.

Tabelle 93: Tab\_gSMC-K\_ObjSys\_182 Initialisierte Attribute von MF / DF.NK / PrK.CFS2.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates Schlüsselobjekt, RSA 2048 |  |
| *keyIdentifier* | ‘0B’ = 11 |  |
| *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]  { signPSS,  rsaDecipherOaep,  rsaDecipherPKCS1\_V1\_5  signPKCS1\_V1\_5,  } |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| **Zugriffsregeln** | | |
| *accessRules* | identisch zu PrK.CFS.R2048 |  |

* + 1. **⌫**

### MF / DF.NK / PrK.CFS.R3072

* + 1. Dieser private Schlüssel für die Kryptographie mit RSA dient ebenfalls herstellerspezifischen Zwecken. Er unterstützt das Signieren und das Entschlüsseln von Daten. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.CFS.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.
    2. Der zugehörige öffent­liche Schlüssel PuK.CFS2.R3072 lässt sich mittels des Kommandos Generate Asymmetric Key Pair (siehe [gem­Spec\_COS#14.9.3.4]) aus diesem Objekt auslesen.
    3. **⌦ Card-G2-A\_3419 K\_Initialisierung: Initialisierte Attribute von MF / DF.NK / PrK.CFS.R3072**
* Das Objekt PrK.CFS.R3072 MUSS die in Tab\_gSMC-K\_ObjSys\_050 dargestellten Werte besitzen.

Tabelle 94: Tab\_gSMC-K\_ObjSys\_050 Initialisierte Attribute von MF / DF.NK / PrK.CFS.R3072

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates Schlüsselobjekt, RSA 3072 |  |
| *keyIdentifier* | ‘13’ = 19 |  |
| *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]  {  signPSS,  rsaDecipherOaep,  rsaDecipherPKCS1\_V1\_5  signPKCS1\_V1\_5,  } |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregeln | | |
| *accessRules* | identisch zu PrK.CFS.R2048 |  |

* + 1. **⌫**

### MF / DF.NK / PrK.CFS.E256

* + 1. Dieser private Schlüssel für die Kryptographie mit elliptischen Kurven dient ebenfalls herstellerspezifischen Zwecken. Er unterstützt das Signieren und das Entschlüsseln von Daten. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.CFS.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.
    2. Der zugehörige öffent­liche Schlüssel PuK.CFS2.E256 lässt sich mittels des Kommandos Generate Asymmetric Key Pair (siehe [gem­Spec\_COS#14.9.3.4]) aus diesem Objekt auslesen.
    3. **⌦ Card-G2-A\_3420 K\_Initialisierung: Initialisierte Attribute von MF / DF.NK / PrK.CFS.E256**
* Das Objekt PrK.CFS.E256 MUSS die in Tab\_gSMC-K\_ObjSys\_183 dargestellten Werte besitzen.

Tabelle 95: Tab\_gSMC-K\_ObjSys\_183 Initialisierte Attribute von MF / DF.NK / PrK.CFS.E256

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates Schlüsselobjekt, ELC 256 |  |
| *keyIdentifier* | ‘0C’ = 12 |  |
| *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]  {elcSharedSecretCalculation, signECDSA} |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregel für logischen LCS „Operational state (activated)” | | |
| *accessRules* | identisch zu PrK.CFS.R2048 |  |

* + 1. **⌫**

### MF / DF.NK / PrK.CFS.E384

* + 1. Dieser private Schlüssel für die Kryptographie mit elliptischen Kurven dient ebenfalls herstellerspezifischen Zwecken. Er unterstützt das Signieren und das Entschlüsseln von Daten. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.CFS.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.
    2. Der zugehörige öffent­liche Schlüssel PuK.CFS2.E384 lässt sich mittels des Kommandos Generate Asymmetric Key Pair (siehe [gem­Spec\_COS#14.9.3.4]) aus diesem Objekt auslesen.
    3. **⌦ Card-G2-A\_3421 K\_Initialisierung: Initialisierte Attribute von MF / DF.NK / PrK.CFS.E384**
* Das Objekt PrK.CFS.E384 MUSS die in Tab\_gSMC-K\_ObjSys\_051 dargestellten Werte besitzen.

Tabelle 96: Tab\_gSMC-K\_ObjSys\_051 Initialisierte Attribute von MF / DF.NK / PrK.CFS.E384

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates Schlüsselobjekt, ELC 384 |  |
| *keyIdentifier* | ‘14’ = 20 |  |
| *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]  {elcSharedSecretCalculation, signECDSA} |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregel für logischen LCS „Operational state (activated)” | | |
| *accessRules* | identisch zu PrK.CFS.R2048 |  |

* + 1. **⌫**

## MF / DF.SAK

* + 1. Die Anwendung DF.SAK enthält kryptographische Objekte der Signaturanwendungskomponente.
    2. Die in dieser Anwendung enthaltenen Schlüssel PrK.SAK.AUT unterstützen den Aufbau eines TLS-Kanals zwischen der SAK und einem Extended Trusted Viewer sowie der SAK zu einem Kartenterminal.
    3. Diese Anwendung enthält für die Kryptographie mit RSA bzw. elliptischen Kurven neben den entsprechenden Schlüsseln korrespondierende Zertifikate, die die zugehörenden öffentlichen Schlüssel PuK.SAK.AUT.XXXX enthalten. Es wird als nicht erforderlich angesehen, dass die Anwendung auch Zertifikate höherer Ebenen enthält.
    4. Mit dem Schlüsselpaar PrK.SAK.SIG.XXXX (mit XXXX aus der Menge {R2048, R3072,. E256, E384) und PuK.SAK.SIG.XXXX (mit XXXX aus der Menge {R2048, R3072,. E256, E384) wird die Erstellung einer Signatur, bzw. Überprüfung einer Signatur für den Integritätsschutz von Konfigurationsdaten der SAK ermöglicht.
    5. Kommunikation mit Karten der Generation 2
    6. Der in dieser Anwendung enthaltene Schlüssel PrK.SAK.AUTD\_CVC.E256 (alternativ PrK.SAK.AUTD\_CVC.E384) für die Kryptographie mit elliptischen Kurven unterstützt den Aufbau eines Trusted Channels zwischen der Signaturanwendungskomponente einerseits und der sicheren Signaturerstellungseinheit andererseits.
    7. Diese Anwendung enthält für die Kryptographie mit elliptischen Kurven neben dem vor­genannten Schlüssel PrK.SAK.AUTD\_CVC.E256 (alternativ PrK.SAK.AUTD\_CVC.E384) ein Zertifikat C.SAK.AUTD\_CVC.E256 (optional C.SAK.AUTD\_CVC.E384), welches den öffentlichen Schlüssel zu PrK.SAK.AUTD\_CVC.E256 (optional PrK.SAK.AUTD\_CVC.E384) enthält. Zur Prü­fung des Zertifikates C.SAK.AUTD\_CVC.E256 (optional C.SAK.AUTD\_CVC.E384) wird der öffentliche Schlüssel aus C.CA\_SAK.CS.E256 (siehe Kapitel 5.3.7) (optional C.CA\_SAK.CS.E384, siehe Kapitel 5.3.9) benötigt.
    8. **⌦ Card-G2-A\_2626 K\_Initialisierung: Vorhandensein von DF.SAK**
* Die Anwendung DF.SAK MUSS auf einer gSMC-K vorhanden sein.
  + 1. **⌫**
    2. **⌦ Card-G2-A\_2627 K\_Initialisierung: Konfiguration von DF.SAK**
* Die Anwendung DF.SAK MUSS gemäß den Angaben dieses Unterkapitels konfiguriert sein.
  + 1. **⌫**
    2. **⌦ Card-G2-A\_2628 K\_Initialisierung: Initialisierte Attribute von MF / DF.SAK**
* Das Objekt DF.SAK MUSS die in Tab\_gSMC-K\_ObjSys\_058 dargestellten Werte besitzen.



Tabelle 97: Tab\_gSMC-K\_ObjSys\_058 Initialisierte Attribute von MF / DF.SAK

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | Ordner |  |
| *applicationIdentifier* | ‘D276 0001 4404’ |  |
| *fileIdentifier* | herstellerspezifisch |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *shareable* | True |  |
| Zugriffsregel für logischen LCS „Operational state (activated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Get Random, | ALWAYS |  |
| Load Application | PWD(PIN.Pers) |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (97) |
| Zugriffsregel für logischen LCS „Termination state“ | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (97) |

* + 1. **⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem Ordnerobjekt arbeiten, sind:   
   Activate, Deactivate, Delete, Fingerprint, Get Random, 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 5.6 im Allgemeinen irrelevant.



Abbildung 4: Abb\_gSMC-K\_ObjSys\_004 Objektstruktur der Anwendung DF.SAK

### MF / DF.SAK / EF.C.SAK.AUT.R2048

* + 1. Diese Zertifikatsdatei ist angelegt, um ein Zertifikat mit dem öffentlichen Schlüssel zu PrK.SAK.AUT.R2048 (siehe Kapitel 5.6.2) aufzunehmen.
    2. **⌦ Card-G2-A\_3422 K\_Initialisierung: Initialisierte Attribute von MF/ DF.SAK / EF.C.SAK.AUT.R2048**
* Das Objekt EF.C.SAK.AUT.R2048 MUSS die in Tab\_gSMC-K\_ObjSys\_167 dargestellten Werte besitzen.

Tabelle 98: Tab\_gSMC-K\_ObjSys\_167 Initialisierte Attribute von MF / DF.SAK / EF.C.SAK.AUT.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ‘C5 06’ |  |
| *shortFileIdentifier* | ’06’ = 6 |  |
| *numberOfOctet* | ‘08 02’ Oktett = 2050 Oktett |  |
| *positionLogicalEndOfFile* | WildCard | 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 (99) |
| Read Binary | ALWAYS |  |
| Set Logical EOF  Write Binary | AUT\_CMS OR AUT\_CUP | siehe Hinweis (99) |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (97) |
| 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. Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.10
   * 1. **⌦ Card-G2-A\_3423 K\_Personalisierung: Personalisierte Attribute von MF/ DF.SAK / EF.C.SAK.AUT.R2048**

* Bei der Personalisierung von EF.C.SAK.AUT.R2048 MÜSSEN die in Tab\_gSMC-K\_ObjSys\_133 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 99: Tab\_gSMC-K\_ObjSys\_133 Attribute von MF / DF.SAK / EF.C.SAK.AUT.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| *positionLogicalEndOfFile* | Zahl der tatsächlich belegten Oktette |  |
| *body* | C.SAK.AUT.R2048 gemäß [gemSpec\_PKI] passend zu dem privaten Schlüssel in PrK.SAK.AUT.R2048 |  |

* + 1. **⌫**

### MF / DF.SAK / PrK.SAK.AUT.R2048

* + 1. Dieses Schlüsselobjekt ist angelegt, um den privaten Schlüssel aufzunehmen, der zu dem öffentlichen Schlüssel in EF.C.SAK.AUT.R2048 gehört.
    2. **⌦ Card-G2-A\_2635 K\_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUT.R2048**
* Das Objekt PrK.SAK.AUT.R2048 MUSS die in Tab\_gSMC-K\_ObjSys\_168 dargestellten Werte besitzen.

Tabelle 100: Tab\_gSMC-K\_ObjSys\_168 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUT.R2048

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute | Wert | Bemerkung | |
| Objekttyp | privates Schlüsselobjekt, RSA 2048 |  | |
| *keyIdentifier* | ‘06’ = 6 |  | |
| *privateKey* | herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Moduluslänge 2048 Bit | wird personalisiert | |
| *keyAvailable* | WildCard |  | |
| *listAlgorithmIdentifier* | Alle Werte aus der Menge sign9796\_2\_DS2, signPKCS1\_V1\_5, signPSS} | siehe  Hinweis (102) | |
| *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=‘81’ | ALWAYS | |  |
| Generate Asymmetric Key Pair  P1=´C4´ oder P1=’C0’ | AUT\_CMS OR AUT\_CUP | | Siehe Hinweis (101) |
| PSO Compute DigitalSignature | PWD(PIN.SAK) | |  |
| Delete | PWD(PIN.SAK)  OR 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. Das Kommando ist nur vom Inhaber des CMS- /CUP-Schlüssels ausführbar, siehe Kapitel 5.10.
3. Wird im Rahmen von Serverauthentisierung für RSA–Ciphersuites verwendet.
4. Wird im Rahmen von Client- und Serverauthentisierung von DH–Ciphersuites verwendet.
   * 1. **⌦ Card-G2-A\_3424 K\_Personalisierung: Personalisierte Attribute von MF / DF.SAK / PrK.SAK.AUT.R2048**

* Bei der Personalisierung von PrK.SAK.AUT.R2048 MÜSSEN die in Tab\_gSMC-K\_ObjSys\_169 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 101: Tab\_gSMC-K\_ObjSys\_169 Attribute von MF / DF.SAK / PrK.SAK.AUT.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| *privateKey* | Moduluslänge 2048 Bit |  |
| *keyAvailable* | True |  |

* + 1. **⌫**

### MF / DF.SAK / EF.C.SAK.AUT2.XXXX

* + 1. Diese Zertifikatsdatei ist angelegt, um ein Zertifikat mit dem öffentlichen Schlüssel PuK.SAK.AUT2.XXXX zu PrK.SAK.AUT2.XXXX (XXXX aus der Menge {R2048, R3072, E256, E384}) nach Ablauf der Nutzungszeit des Schlüssels PrK.SAK.AUT.R2048 aufzunehmen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.
    2. **⌦ Card-G2-A\_2631 K\_Initialisierung: Initialisierte Attribute von MF/ DF.SAK / EF.C.SAK.AUT2.XXXX**
* Das Objekt EF.C.SAK.AUT2.XXXX MUSS bei Ausgabe der Karte mit den in Tab\_gSMC-K\_ObjSys\_060 dargestellten Werten angelegt werden.

Tabelle 102: Tab\_gSMC-K\_ObjSys\_060 Initialisierte Attribute von MF / DF.SAK / EF.C.SAK.AUT2.XXXX

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ‘C5 07’ |  |
| *shortFileIdentifier* | ’07’ = 7 |  |
| *numberOfOctet* | ‘08 02’ Oktett = 2.050 Oktett |  |
| *positionLogicalEndOfFile* | ’0’ |  |
| *flagTransactionMode* | True |  |
| *flagChecksum* | False |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *shareable* | True |  |
| *body* | kein Inhalt | wird später nachgeladen |
| Zugriffsregel für logischen LCS „Operational state (activated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Delete | AUT\_CMS OR AUT\_CUP | siehe Hinweis (105) |
| Read Binary | ALWAYS |  |
| Set Logical EOF  Write Binary | AUT\_CMS OR AUT\_CUP | siehe Hinweis (105) |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (97) |
| 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. Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.10

### MF / DF.SAK / PrK.SAK.AUT2.R2048

* + 1. Dieses Schlüsselobjekt ist angelegt, um den privaten Schlüssel aufzunehmen, der zu dem öffentlichen Schlüssel in EF.C.SAK.AUT2.XXXX gehört. Es stellt eine der Möglichkeiten dar, den Schlüssel PrK.SAK.AUT.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.
    2. **⌦ Card-G2-A\_3425 K\_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUT2.R2048**
* Das Objekt PrK.SAK.AUT2.R2048 MUSS die in Tab\_gSMC-K\_ObjSys\_170 dargestellten Werte besitzen.

Tabelle 103: Tab\_gSMC-K\_ObjSys\_170 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUT2.R2048

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute | Wert | Bemerkung | |
| Objekttyp | privates Schlüsselobjekt, RSA 2048 |  | |
| *keyIdentifier* | ‘07’ = 7 |  | |
| *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  {sign9796\_2\_DS2, signPKCS1\_V1\_5, signPSS} | siehe  Hinweis (107) | |
| *lifeCycleStatus* | „Operational state (activated)“ |  | |
| Zugriffsregeln | | | |
| *accessRules* | identisch zu PrK.SAK.AUT.R2048 | |  |

* + 1. **⌫**

1. Wird im Rahmen von Serverauthentisierung für RSA–Ciphersuites verwendet.
2. Wird im Rahmen von Client- und Serverauthentisierung von DH–Ciphersuites verwendet.

### MF / DF.SAK / PrK.SAK.AUT.R3072

* + 1. Dieses Schlüsselobjekt ist angelegt, um den privaten Schlüssel aufzunehmen, der zu dem öffentlichen Schlüssel in EF.C.SAK.AUT2.XXXX gehört. Es stellt eine der Möglichkeiten dar, den Schlüssel PrK.SAK.AUT.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.
    2. **⌦ Card-G2-A\_3426 K\_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUT.R3072**
* Das Objekt PrK.SAK.AUT.R3072 MUSS die in Tab\_gSMC-K\_ObjSys\_171 dargestellten Werte besitzen.

Tabelle 104: Tab\_gSMC-K\_ObjSys\_171 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUT.R3072

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute | Wert | Bemerkung | |
| Objekttyp | privates Schlüsselobjekt, RSA 3072 |  | |
| *keyIdentifier* | 08’ = 8 |  | |
| *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  {sign9796\_2\_DS2, signPKCS1\_V1\_5, signPSS} | siehe  Hinweis (109) | |
| *lifeCycleStatus* | „Operational state (activated)“ |  | |
| Zugriffsregeln | | | |
| *accessRules* | identisch zu PrK.SAK.AUT.R2048 | |  |

* + 1. **⌫**

1. Wird im Rahmen von Serverauthentisierung für RSA–Ciphersuites verwendet.
2. Wird im Rahmen von Client- und Serverauthentisierung von DH–Ciphersuites verwendet.

### MF / DF.SAK / PrK.SAK.AUT.E256

* + 1. Dieses Schlüsselobjekt ist angelegt, um den privaten Schlüssel aufzunehmen, der zu dem öffentlichen Schlüssel in EF.C.SAK.AUT2.XXXX gehört. Es stellt eine der Möglichkeiten dar, den Schlüssel PrK.SAK.AUT.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.
    2. **⌦ Card-G2-A\_3427 K\_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUT.E256**
* Das Objekt PrK.SAK.AUT.E256 MUSS die in Tab\_gSMC-K\_ObjSys\_172 dargestellten Werte besitzen.

Tabelle 105: Tab\_gSMC-K\_ObjSys\_172 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUT.E256

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute | Wert | Bemerkung | |
| Objekttyp | privates Schlüsselobjekt, ELC 256 |  | |
| *keyIdentifier* | ‘05’ = 5 |  | |
| *privateElcKey* | domainparameter = brainpoolP256r1 | wird später mit Generate Asymmetric Key Pair erzeugt | |
| *privateElcKey* | keyData = AttributNotSet |  | |
| *keyAvailable* | False |  | |
| *listAlgorithmIdentifier* | signECDSA |  | |
| *lifeCycleStatus* | „Operational state (activated)“ |  | |
| Zugriffsregeln | | | |
| *accessRules* | identisch zu PrK.SAK.AUT.R2048 | |  |

* + 1. **⌫**

### MF / DF.SAK / PrK.SAK.AUT.E384

* + 1. Dieses Schlüsselobjekt ist angelegt, um den privaten Schlüssel aufzunehmen, der zu dem öffentlichen Schlüssel in EF.C.SAK.AUT2.XXXX gehört. Es stellt eine der Möglichkeiten dar, den Schlüssel PrK.SAK.AUT.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen.
    2. **⌦ Card-G2-A\_3428 K\_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUT.E384**
* Das Objekt PrK.SAK.AUT.E384 MUSS die in Tab\_gSMC-K\_ObjSys\_173 dargestellten Werte besitzen.

Tabelle 106: Tab\_gSMC-K\_ObjSys\_173 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUT.E384

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute | Wert | Bemerkung | |
| Objekttyp | privates Schlüsselobjekt, ELC 384 |  | |
| *keyIdentifier* | ‘09’ = 9 |  | |
| *privateElcKey* | domainparameter = brainpoolP384r1 | wird später mit Generate Asymmetric Key Pair erzeugt | |
| *privateElcKey* | keyData = AttributNotSet |  | |
| *keyAvailable* | False |  | |
| *listAlgorithmIdentifier* | signECDSA |  | |
| *lifeCycleStatus* | „Operational state (activated)“ |  | |
| Zugriffsregeln | | | |
| *accessRules* | identisch zu PrK.SAK.AUT.R2048 | |  |

* + 1. **⌫**

### MF / DF.SAK / EF.C.SAK.AUTD\_CVC.E256

* + 1. EF.C.SAK.AUTD\_CVC.E256 enthält ein CV–Zertifikat gemäß [gemSpec\_COS], welches den öffentlichen Schlüssel PuK.SAK.AUTD\_CVC.E256 enthält. Dieses Zertifikat lässt sich mittels des öffentlichen Schlüssels aus EF.C.CA\_SAK.CS.E256 (siehe Kapitel 5.3.8) prüfen.
    2. **⌦ Card-G2-A\_2638 K\_Personalisierung: CHR von C.SAK.AUTD\_CVC.E256**
* Für die CHR des Zertifikates MUSS gelten: CHR = ‘00 0A’ || ICCSN, wobei die ICCSN denselben Wert besitzen MUSS wie das Wertfeld *body* aus Card-G2-A\_2567).
  + 1. **⌫**
    2. **⌦ Card-G2-A\_2639 K\_Initialisierung: Initialisierte Attribute von MF / DF.SAK / EF.C.SAK.AUTD\_CVC.E256**
* Das Objekt EF.C.SAK.AUTD\_CVC.E256 MUSS die in Tab\_gSMC-K\_ObjSys\_064 dargestellten Werte besitzen.

Tabelle 107: Tab\_gSMC-K\_ObjSys\_064 Initialisierte Attribute von MF / DF.SAK / EF.C.SAK.AUTD\_CVC.E256

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ‘2F 0A’ |  |
| *shortFileIdentifier* | ‘0A’ = 10 |  |
| *numberOfOctet* | ‘011F’ Oktett = 287 Oktett |  |
| *positionLogicalEndOfFile* | WildCard | wird personalisiert |
| *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 (111) |
| Read Binary | ALWAYS |  |
| Set Logical EOF  Write Binary | AUT\_CMS OR AUT\_CUP | siehe Hinweis (111) |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (97) |
| Zugriffsregel für logischen LCS „Termination state“ | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (97) |

* + 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 5.10
   * 1. **⌦ Card-G2-A\_3429 K\_Personalisierung: Personalisierte Attribute von MF / DF.SAK / EF.C.SAK.AUTD\_CVC.E256**

* Bei der Personalisierung von EF.C.SAK.AUTD\_CVC.E256 MÜSSEN die in Tab\_gSMC-K\_ObjSys\_135 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 108: Tab\_gSMC-K\_ObjSys\_135 Attribute von MF / DF.SAK / EF.C.SAK.AUTD\_CVC.E256

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| *positionLogicalEndOfFile* | ‘00DE’ Oktett = 222 Oktett |  |
| *body* | C.SAK.AUTD\_CVC.E256 gemäß [gemSpec\_PKI] passend zu dem privaten Schlüssel in PrK.SAK.AUTD\_CVC.E256 |  |

**⌫**

### MF / DF.SAK / PrK.SAK.AUTD\_CVC.E256

* + 1. PrK.SAK.AUTD\_CVC.E256 wird im Rahmen von asymmetrischen Authentisierungsprotokollen für die Kryptographie mit elliptischen Kurven verwendet. Der zugehörige öffentliche Schlüssel PuK.SAK.AUTD\_CVC.E256 ist in C.SAK.AUTD\_CVC.E256 (siehe Kapitel 5.6.8) enthalten.
    2. **⌦ Card-G2-A\_2643 K\_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUTD\_CVC.E256**
* Die Objekte PrK.SAK.AUTD\_CVC.E256 MÜSSEN die in Tab\_gSMC-K\_ObjSys\_067 dargestellten Werte besitzen.

Tabelle 109: Tab\_gSMC-K\_ObjSys\_067 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUTD\_CVC.E256

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates Schlüsselobjekt ELC 256 |  |
| *keyIdentifier* | ‘0A’ = 10 |  |
| *privateElcKey* | *domainparameter = brainpoolP256r1* |  |
| *privateElcKey* | *keyData = AttributNotSet* | *wird personalisiert* |
| *keyAvailable* | WildCard |  |
| *listAlgorithmIdentifier* | alle Werte aus der Menge { elcSessionkey4TC} |  |
| *accessRulesSessionkeys* | Für alle logischen LCS Werte gilt  Zugriffsart = PSO  🡪 Zugriffsbedingung = AUT(flagTI.52) |  |
| lifeCycleStatus | „Operational state (activated)“ |  |
| Zugriffsregel für logischen LCS „Operational state (activated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Activate  Deactivate | AUT\_CMS OR AUT\_CUP |  |
| Generate Asymmetric Key Pair  P1=´C4´ oder P1=’C0’ | AUT\_CMS OR AUT\_CUP | siehe Hinweis (114) |
| Generate Asymmetric Key Pair  P1=‘81’ | PWD(PIN.SAK) |  |
| General Authenticate | ALWAYS | siehe Hinweis (113) |
| Delete | AUT\_CMS OR AUT\_CUP | siehe Hinweis (114) |
| Andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Alle | herstellerspezifisch | siehe Hinweis (97) |
| Zugriffsregel für logischen LCS „Termination state“ | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Alle | NEVER |  |

* + 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. Diese Rolle ist einem HBA zugewiesen
3. Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.10.
   * 1. **⌦ Card-G2-A\_3430 K\_Personalisierung: Personalisierte Attribute von MF / DF.SAK / PrK.SAK.AUTD\_CVC.E256**

* Die Objekte PrK.SAK.AUTD\_CVC.E256 MÜSSEN die in Tab\_gSMC-K\_ObjSys\_137 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 110: Tab\_gSMC-K\_ObjSys\_137 Attribute von MF / DF.SAK / PrK.SAK.AUTD\_CVC.E256

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| *keyAvailable* | True |  |
| privateElcKey | keyData = eine ganze Zahl im Intervall [1, domainParameter.n – 1] |  |

* + 1. **⌫**

### MF / DF.SAK / EF.C.SAK.AUTD\_CVC.E384

* + 1. EF.C.SAK.AUTD\_CVC.E384 enthält ein CV–Zertifikat gemäß [gemSpec\_COS], welches den öffentlichen Schlüssel PuK.SAK.AUTD\_CVC.E384 enthält. Dieses Zertifikat lässt sich mittels des öffentlichen Schlüssels aus EF.C.CA\_SAK.CS.E384 (siehe Kapitel 5.3.9 prüfen.
    2. **⌦ Card-G2-A\_2640 K\_Personalisierung: CHR von C.SAK.AUTD\_CVC.E384**
* Für die CHR des Zertifikates MUSS gelten: CHR = ‘00 0F’ || ICCSN, wobei die ICCSN denselben Wert besitzen MUSS wie das Wertfeld *body* aus Card-G2-A\_2567).
  + 1. **⌫**
    2. **⌦ Card-G2-A\_2641 K\_Initialisierung: Initialisierte Attribute von MF / DF.SAK / EF.C.SAK.AUTD\_CVC.E384**
* Das Objekt EF.C.SAK.AUTD\_CVC.E384 MUSS die in Tab\_gSMC-K\_ObjSys\_065 dargestellten Werte besitzen.

Tabelle 111: Tab\_gSMC-K\_ObjSys\_065 Initialisierte Attribute von MF / DF.SAK / EF.C.SAK.AUTD\_CVC.E384

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ‘2F 0F’ |  |
| *shortFileIdentifier* | ‘0F’ = 15 |  |
| *numberOfOctet* | ‘011F’ 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.SAK.AUTD\_CVC.E256 | siehe Hinweis (97) |

* + 1. **⌫**

### MF / DF.SAK / PrK.SAK.AUTD\_CVC.E384

* + 1. PrK.SAK.AUTD\_CVC.E384 wird im Rahmen von asymmetrischen Authentisierungsprotokollen für die Kryptographie mit elliptischen Kurven verwendet. Der zugehörige öffentliche Schlüssel PuK.SAK.AUTD\_CVC.E384 ist in C.SAK.AUTD\_CVC.E384 (siehe Kapitel 5.6.10) enthalten.
    2. **⌦ Card-G2-A\_2644 K\_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUTD\_CVC.E384**
* Das Objekt PrK.SAK.AUTD\_CVC.E384 MUSS die in Tab\_gSMC-K\_ObjSys\_068 dargestellten Werte besitzen.

Tabelle 112: Tab\_gSMC-K\_ObjSys\_068 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUTD\_CVC.E384

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates Schlüsselobjekt ELC 384 |  |
| *keyIdentifier* | ‘0F’ = 15 |  |
| *privateElcKey* | domainparameter = brainpoolP384r1 | wird später mit Generate Asymmetric Key Pair erzeugt |
| *privateElcKey* | keyData = AttributNotSet |  |
| *keyAvailable* | False |  |
| *listAlgorithmIdentifier* | alle Werte aus der Menge {elcSessionkey4TC} |  |
| *accessRulesSessionkeys* | identisch zu PrK.SAK.AUTD\_CVC.E256 |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregeln | | |
| *accessRules* | identisch zu PrK.SAK.AUTD\_CVC.E256 |  |

* + 1. **⌫**

### MF / DF.SAK / PrK.SAK.CA\_xTV.R2048

* + 1. Dieser private CA-Schlüssel für die Kryptographie mit RSA dient herstellerspezifischen Zwecken im Bereich des Extended Trusted Viewers. Mit diesem Schlüssel können X.509-Zertifikate für einen Trusted Viewer signiert werden. Der zugehörige öffentliche Schlüssel lässt sich auch mittels des Kommandos Generate Asymmetric Key Pair (siehe [gemSpec\_COS#14.9.3.4]) auslesen.
    2. **⌦ Card-G2-A\_2645 K\_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.CA\_xTV.R2048**
* Das Objekt PrK.SAK.CA\_xTV.R2048 MUSS die in Tab\_gSMC-K\_ObjSys\_069 dargestellten Werte besitzen.

Tabelle 113: Tab\_gSMC-K\_ObjSys\_069 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.CA\_xTV.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates Schlüsselobjekt, RSA 2048 |  |
| *keyIdentifier* | ‘0B’ = 11 |  |
| *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]  {sign9796\_2\_DS2, signPKCS1\_V1\_5, signPSS} |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregel für logischen LCS „Operational state (activated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Generate Asymmetric Key Pair  P1=‘84’oder P1=’80’ | PWD(PIN.SAK) |  |
| Generate Asymmetric Key Pair  P1=‘81’ | ALWAYS |  |
| PSO CompDigSig | PWD(PIN.SAK) |  |
| Terminate | PWD(PIN.SAK) |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (97) |
| 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. Die Zugriffsbedingung wird in Abstimmung mit den Konnektorherstellern noch festgelegt
   * 1. **⌦ Card-G2-A\_3431 K\_Personalisierung: Personalisierte Attribute von MF / DF.SAK / PrK.SAK.CA\_xTV.R2048**

* Bei der Personalisierung von PrK.SAK.CA\_xTV.R2048 MÜSSEN die in Tab\_gSMC-K\_ObjSys\_139 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 114: Tab\_gSMC-K\_ObjSys\_139 Attribute von MF / DF.SAK / PrK.SAK.CA\_xTV.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| *privateKey* | Moduluslänge 2048 Bit |  |
| *keyAvailable* | True |  |

* + 1. **⌫**

### MF / DF.SAK / PrK.SAK.CA\_xTV2.R2048

* + 1. Dieser private Schlüssel für die Kryptographie mit RSA dient ebenfalls herstellerspezifischen Zwecken im Bereich des Extended Trusted Viewers; mit diesem Schlüssel können X.509-Zertifikate für einen Trusted Viewer signiert werden. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.SAK.CA\_xTV.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen. Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos Generate Asymmetric Key Pair (siehe [gemSpec\_COS#14.9.3.4]) auslesen.
    2. **⌦ Card-G2-A\_3432 K\_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.CA\_xTV2.R2048**
* Das Objekt PrK.SAK.CA\_xTV2.R2048 MUSS die in Tab\_gSMC-K\_ObjSys\_174 dargestellten Werte besitzen.

Tabelle 115: Tab\_gSMC-K\_ObjSys\_174 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.CA\_xTV2.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates Schlüsselobjekt, RSA 2048 |  |
| *keyIdentifier* | ‘19’ = 25 |  |
| *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]  {sign9796\_2\_DS2, signPKCS1\_V1\_5, signPSS} |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregeln | | |
| *accessRules* | identisch zu PrK.SAK.CA\_xTV.R2048 |  |

* + 1. **⌫**

### MF / DF.SAK / PrK.SAK.CA\_xTV.R3072

* + 1. Dieser private Schlüssel für die Kryptographie mit RSA dient ebenfalls herstellerspezifischen Zwecken im Bereich des Extended Trusted Viewers; mit diesem Schlüssel können X.509-Zertifikate für einen Trusted Viewer signiert werden.. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.SAK.CA\_xTV.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen. Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos Generate Asymmetric Key Pair (siehe [gemSpec\_COS#14.9.3.4]) auslesen.
    2. **⌦ Card-G2-A\_2646 K\_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.CA\_xTV.R3072**
* Das Objekt PrK.SAK.CA\_xTV.R3072 MUSS die in Tab\_gSMC-K\_ObjSys\_070 dargestellten Werte besitzen.

Tabelle 116: Tab\_gSMC-K\_ObjSys\_070 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.CA\_xTV.R3072

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates Schlüsselobjekt, RSA 3072 |  |
| *keyIdentifier* | ‘0C’ = 12 |  |
| 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]  {sign9796\_2\_DS2, signPKCS1\_V1\_5, signPSS} |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregeln | | |
| *accessRules* | identisch zu PrK.SAK.CA\_xTV.R2048 |  |

* + 1. **⌫**

### MF / DF.SAK / PrK.SAK.CA\_xTV.E256

* + 1. Dieser private Schlüssel für die Kryptographie mit elliptischen Kurven dient ebenfalls herstellerspezifischen Zwecken im Bereich des Extended Trusted Viewers; mit diesem Schlüssel können X.509-Zertifikate für einen Trusted Viewer signiert werden.. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.SAK.CA\_xTV.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen. Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos Generate Asymmetric Key Pair (siehe [gemSpec\_COS#14.9.3.4]) auslesen.
    2. **⌦ Card-G2-A\_3433 K\_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.CA\_xTV.E256**
* Das Objekt PrK.SAK.CA\_xTV.E256 MUSS die in Tab\_gSMC-K\_ObjSys\_184 dargestellten Werte besitzen.

Tabelle 117: Tab\_gSMC-K\_ObjSys\_184 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.CA\_xTV.E256

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates Schlüsselobjekt, ELC 256 |  |
| *keyIdentifier* | ‘0E’ = 14 |  |
| *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]  {signECDSA} |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregeln | | |
| *accessRules* | identisch zu PrK.SAK.CA\_xTV.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

### MF / DF.SAK / PrK.SAK.CA\_xTV.E384

* + 1. Dieser private Schlüssel für die Kryptographie mit elliptischen Kurven dient ebenfalls herstellerspezifischen Zwecken im Bereich des Extended Trusted Viewers; mit diesem Schlüssel können X.509-Zertifikate für einen Trusted Viewer signiert werden. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.SAK.CA\_xTV.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen. Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos Generate Asymmetric Key Pair (siehe [gemSpec\_COS#14.9.3.4]) auslesen.
    2. **⌦ Card-G2-A\_2647 K\_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.CA\_xTV.E384**
* Das Objekt PrK.SAK.CA\_xTV.E384 MUSS die in Tab\_gSMC-K\_ObjSys\_071 dargestellten Werte besitzen.

Tabelle 118: Tab\_gSMC-K\_ObjSys\_071 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.CA\_xTV.E384

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates Schlüsselobjekt, ELC 384 |  |
| *keyIdentifier* | ‘0D’ = 13 |  |
| *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]  {signECDSA} |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregeln | | |
| *accessRules* | identisch zu PrK.SAK.CA\_xTV.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

### MF / DF.SAK / PrK.SAK.SIG.R2048

* + 1. Dieser private Schlüssel für die Kryptographie mit RSA dient dazu Konfigurationsdaten der SAK zu signieren mit dem Ziel die Integrität der Daten zu schützen. Da es sich um eine SAK interne Funktionalität handelt, ist ein Zertifikat nicht erforderlich.
    2. Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos Generate Asymmetric Key Pair (siehe [gemSpec\_COS#14.9.3.4]) auslesen.
    3. **⌦ Card-G2-A\_2648 K\_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.SIG.R2048**
* Das Objekt PrK.SAK.SIG.R2048 MUSS die in Tab\_gSMC-K\_ObjSys\_072 dargestellten Werte besitzen.

Tabelle 119: Tab\_gSMC-K\_ObjSys\_072 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.SIG.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates Schlüsselobjekt, RSA 2048 |  |
| *keyIdentifier* | ‘14’ = 20 |  |
| *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]  {sign9796\_2\_DS2, signPSS} |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregel für logischen LCS „Operational state (activated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Generate Asymmetric Key Pair  P1=‘84’ oder P1=’80’ | PWD(PIN.SAK) |  |
| Generate Asymmetric Key Pair  P1=‘81’ | ALWAYS |  |
| PSO CompDigSig | PWD(PIN.SAK) |  |
| Terminate | PWD(PIN.SAK) |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (97) |
| 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. Die Zugriffsbedingung wird in Abstimmung mit den Konnektorherstellern noch festgelegt
   * 1. **⌦ Card-G2-A\_3434 K\_Personalisierung: Personalisierte Attribute von MF / DF.SAK / PrK.SAK.SIG.R2048**

* Bei der Personalisierung von PrK.SAK.SIG.R2048 MÜSSEN die in Tab\_gSMC-K\_ObjSys\_142 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 120: Tab\_gSMC-K\_ObjSys\_142 Attribute von MF / DF.SAK / PrK.SAK.SIG.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| *privateKey* | Moduluslänge 2048 Bit |  |
| *keyAvailable* | True |  |

* + 1. **⌫**

### MF / DF.SAK / PrK.SAK.SIG2.R2048

* + 1. Dieser private Schlüssel für die Kryptographie mit RSA dient ebenfalls dazu, Konfigurationsdaten der SAK zu signieren mit dem Ziel, die Integrität der Daten zu schützen. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.SAK.SIG.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen. Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos Generate Asymmetric Key Pair (siehe [gemSpec\_COS#14.9.3.4]) auslesen.
    2. Da es sich um eine SAK interne Funktionalität handelt, ist ein Zertifikat nicht erforderlich.
    3. **⌦ Card-G2-A\_3435 K\_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.SIG2.R2048**
* Das Objekt PrK.SAK.SIG2.R2048 MUSS die in Tab\_gSMC-K\_ObjSys\_185 dargestellten Werte besitzen.

Tabelle 121: Tab\_gSMC-K\_ObjSys\_185 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.SIG2.R2048

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates Schlüsselobjekt, RSA 2048 |  |
| *keyIdentifier* | ‘17’ = 23 |  |
| *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]  {sign9796\_2\_DS2, signPSS} |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregeln | | |
| *accessRules* | identisch zu PrK.SAK.SIG.R2048 |  |

* + 1. **⌫**

### MF / DF.SAK / PrK.SAK.SIG.R3072

* + 1. Dieser private Schlüssel für die Kryptographie mit RSA dient ebenfalls dazu, Konfigurationsdaten der SAK zu signieren mit dem Ziel, die Integrität der Daten zu schützen. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.SAK.SIG.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen. Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos Generate Asymmetric Key Pair (siehe [gemSpec\_COS#14.9.3.4]) auslesen.
    2. Da es sich um eine SAK interne Funktionalität handelt, ist ein Zertifikat nicht erforderlich.
    3. **⌦ Card-G2-A\_2649 K\_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.SIG.R3072**
* Das Objekt PrK.SAK.SIG.R3072 MUSS die in Tab\_gSMC-K\_ObjSys\_073 dargestellten Werte besitzen.

Tabelle 122: Tab\_gSMC-K\_ObjSys\_073 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.SIG.R3072

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates Schlüsselobjekt, RSA 3072 |  |
| *keyIdentifier* | ’15’ = 21 |  |
| *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]  {sign9796\_2\_DS2, signPSS} |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregeln | | |
| *accessRules* | identisch zu PrK.SAK.SIG.R2048 |  |

* + 1. **⌫**

### MF / DF.SAK / PrK.SAK.SIG.E256

* + 1. Dieser private Schlüssel für die Kryptographie mit elliptischen Kurven dient ebenfalls dazu, Konfigurationsdaten der SAK zu signieren mit dem Ziel, die Integrität der Daten zu schützen. Er stellt eine der Möglichkeiten dar, den Schlüssel PrK.SAK.SIG.R2048 nach Ablauf seiner Nutzungszeit abzulösen. Die Entscheidung, welches Verfahren aus der Menge {R2048, R3072, E256, E384} bei einem Wechsel des Schlüsselmaterials gewählt wird, wird zu einem späteren Zeitpunkt getroffen. Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos Generate Asymmetric Key Pair (siehe [gemSpec\_COS#14.9.3.4]) auslesen.
    2. Da es sich um eine SAK interne Funktionalität handelt, ist ein Zertifikat nicht erforderlich.
    3. **⌦ Card-G2-A\_3436 K\_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.SIG.E256**
* Das Objekt PrK.SAK.SIG.E256 MUSS die in Tab\_gSMC-K\_ObjSys\_186 dargestellten Werte besitzen.

Tabelle 123: Tab\_gSMC-K\_ObjSys\_186 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.SIG.E256

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates Schlüsselobjekt, ELC 256 |  |
| *keyIdentifier* | ’18’ = 24 |  |
| *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]  {signECDSA } |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregel für logischen LCS „Operational state (activated)” | | |
| *accessRules* | identisch zu PrK.SAK.SIG.R2048 |  |

* + 1. **⌫**

### MF / DF.SAK / PrK.SAK.SIG.E384

* + 1. Dieser private Schlüssel für die Kryptographie mit elliptischen Kurven dient dazu Konfigurationsdaten der SAK zu signieren mit dem Ziel die Integrität der Daten zu schützen. Da es sich um eine SAK interne Funktionalität handelt, ist ein Zertifikat nicht erforderlich.
    2. Der zugehörige öffentliche Schlüssel lässt sich mittels des Kommandos Generate Asymmetric Key Pair (siehe [gemSpec\_COS#14.9.3.4]) auslesen.
    3. **⌦ Card-G2-A\_2650 K\_Initialisierung: Initialisierte Attribute von MF / DF.SAK / PrK.SAK.SIG.E384**
* Das Objekt PrK.SAK.SIG.E384 MUSS die in Tab\_gSMC-K\_ObjSys\_074 dargestellten Werte besitzen.

Tabelle 124: Tab\_gSMC-K\_ObjSys\_074 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.SIG.E384

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | privates Schlüsselobjekt, ELC 384 |  |
| *keyIdentifier* | ’16’ = 22 |  |
| *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]  {signECDSA } |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregel für logischen LCS „Operational state (activated)” | | |
| *accessRules* | identisch zu PrK.SAK.SIG.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

## MF / DF.Sicherheitsanker

* + 1. Die Anwendung DF.Sicherheitsanker enthält Zertifikate, die im Rahmen der Prüfung von TSL- oder TCL-Listen und QES-Zertifikaten relevant sind.

1. Aktuell werden in diesem Ordner Root Zertifikate C.TSL.CA gespeichert. Diese selbstsignierten Zertifikate enthalten einen öffentlichen Schlüssel zur Prüfung der Signer Zertifikate C.TSL.SIG und C.TCL.SIG. Die öffentlichen Schlüssel der letztgenannten Signaturzertifikate dienen dazu, Signaturen von TSL bzw. TCL Listen zu prüfen.

* + 1. **⌦ Card-G2-A\_2653 K\_Initialisierung: Initialisierte Attribute von MF / DF.Sicherheitsanker**
* Das Objekt DF.Sicherheitsanker MUSS die in Tab\_gSMC-K\_ObjSys\_075 dargestellten Werte besitzen.

Tabelle 125: Tab\_gSMC-K\_ObjSys\_075 Initialisierte Attribute von MF / DF.Sicherheitsanker

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | Ordner |  |
| *applicationIdentifier* | ‘D276 0001 4405’ |  |
| *fileIdentifier* | herstellerspezifisch |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *shareable* | True |  |
| Zugriffsregel für logischen LCS „Operational state (activated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Get Random | ALWAYS |  |
| Load Application | PWD(PIN.Pers) |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (124) |
| Zugriffsregel für logischen LCS „Termination state“ | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (124) |

* + 1. **⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem Ordnerobjekt arbeiten, sind:   
   Activate, Deactivate, Delete, Fingerprint, Get Random, 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 5.7 im Allgemeinen irrelevant.



Abbildung 5: Abb\_gSMC-K\_ObjSys\_005 Dateistruktur der Anwendung DF.Sicherheitsanker

### MF / DF.Sicherheitsanker / EF.C.BNetzA.RCA

* + 1. Diese Datei enthält ein Zertifikat mit dem öffentlichen Schlüssel PuK.BnetzA.RCA. Dieser öffentliche Schlüssel dient der Verifikation des Zertifikates C.BnetzA.RCA, welches ein selbstsigniertes Wurzelzertifikat der Bundesnetzagentur ist. Falls der Fehlbedienungszähler *retryCounter* von PIN.BNetzA\_RCA den Wert null besitzt, dann sind weitere Änderungen des Dateiinhaltes unmöglich.
    2. **⌦ Card-G2-A\_2654 K\_Initialisierung: Initialisierte Attribute von MF / DF.Sicherheitsanker / EF.C.BNetzA.RCA**
* Das Objekt EF.C.BNetzA.RCA MUSS die in Tab\_gSMC-K\_ObjSys\_076 dargestellten Werte besitzen.

Tabelle 126: Tab\_gSMC-K\_ObjSys\_076 Initialisierte Attribute von MF / DF.Sicherheitsanker / EF.C.BNetzA.RCA

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ‘C6 10’ |  |
| *shortFileIdentifier* | ‘10’ = 16 |  |
| *numberOfOctet* | ‘08 02’ Oktett = 2.050 Oktett |  |
| positionLogicalEndOfFile | Zahl der tatsächlich belegten Oktette |  |
| *flagTransactionMode* | True |  |
| *flagChecksum* | False |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *shareable* | True |  |
| Für Echtkarten MUSS das nachfolgende Attribut mit dem unten angegebenen Wert initialisiert werden.  Für Option\_Erstellung\_von\_Testkarten MUSS das nachfolgende Attribut mit Wildcard oder AttributeNotSet initialisiert werden. | | |
| body | ‘  Aktuelles Root-Zertifikat der BNetzA (C.BNetzA.RCA) gemäß [gemSpec\_PKI#8.5.2] |  |
| Zugriffsregel für logischen LCS „Operational state (activated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Read Binary | ALWAYS |  |
| Erase Binary  Set Logical EOF  Update Binary  Write Binary | PWD(PIN.BnetzA\_RCA) |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (124) |
| Zugriffsregel für logischen LCS „Termination state“ | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (124) |

* + 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. **⌦ Card-G2-A\_3582 K\_Personalisierung: Personalisierte Attribute von MF / EF.C.BNetzA.RCA für Testkarten**

* Bei der Personalisierung von EF.C.BNetzA.RCA für Testkarten MUSS das in Tab\_gSMC-K\_ObjSys\_214 angegebene Attribut mit dem dort angegebenen Inhalt personalisiert werden.

Tabelle 127: Tab\_gSMC-K\_ObjSys\_214 Personalisierte Attribute von MF / EF.C.BNetzA.RCA für Testkarten

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| *body* | Root-Zertifikat der Pseudo-QES-Root gemäß [gemSpec\_PKI#8.5.2] |  |

* + 1. **⌫**

### MF / DF.Sicherheitsanker / EF.C.TSL.CA\_1

* + 1. Genau wie EF.C.TSL.CA\_2 in Kapitel 5.7.3 enthält diese Datei ein Zertifikat mit dem öffentlichen Schlüssel PuK.TSL.CA\_1. Dieser öffentliche Schlüssel dient der Verifikation des Zertifikates C.TSL.SIG. Bei C.TSL.CA\_1 handelt es sich um ein CA-Zertifikat. Falls der Fehlbedienungszähler *retryCounter* von PIN.TSL\_CA\_1 den Wert null besitzt, dann sind weitere Änderungen des Dateiinhaltes unmöglich.
    2. **⌦ Card-G2-A\_2655 K\_Initialisierung: Initialisierte Attribute von MF / DF.Sicherheitsanker / EF.C.TSL.CA\_1**
* Das Objekt EF.C.TSL.CA\_1 MUSS die in Tab\_gSMC-K\_ObjSys\_077 dargestellten Werte besitzen.

Tabelle 128: Tab\_gSMC-K\_ObjSys\_077 Initialisierte Attribute von MF / DF.Sicherheitsanker / EF.C.TSL.CA\_1

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ‘C6 01’ |  |
| *shortFileIdentifier* | ‘01’ = 1 |  |
| *numberOfOctet* | ‘08 02’ Oktett = 2050 Oktett |  |
| positionLogicalEndOfFile | Zahl der tatsächlich belegten Oktette |  |
| *flagTransactionMode* | True |  |
| *flagChecksum* | False |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *shareable* | True |  |
| Für Echtkarten MUSS das nachfolgende Attribut mit dem unten angegebenen Wert initialisiert werden.  Für Option\_Erstellung\_von\_Testkarten MUSS das nachfolgende Attribut mit Wildcard oder AttributeNotSet initialisiert werden. | | |
| body | C.TSL.CA\_1 gemäß [gemSpec\_PKI#5.13.3] |  |
| Zugriffsregel für logischen LCS „Operational state (activated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Read Binary | ALWAYS |  |
| Erase Binary  Set Logical EOF  Update Binary  Write Binary | PWD(PIN.TSL\_CA) |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (124) |
| Zugriffsregel für logischen LCS „Termination state“ | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (124) |

* + 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. **⌦ Card-G2-A\_3583 K\_Personalisierung: Personalisierte Attribute von MF / EF.C.TSL.CA\_1 für Testkarten**

* Bei der Personalisierung von EF.C.TSL.CA\_1 für Testkarten MUSS das in Tab\_gSMC-K\_ObjSys\_215 angegebene Attribut mit dem dort angegebenen Inhalt personalisiert werden.

Tabelle 129: Tab\_gSMC-K\_ObjSys\_215 Personalisierte Attribute von MF / EF.C.TSL.CA\_1 für Testkarten

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Wert** | **Bemerkung** |
| *body* | Zertifikat der Test-TSL.CA gemäß gemSpec\_PKI[gemSpec\_PKI#5.13.3] |  |

* + 1. **⌫**

### MF / DF.Sicherheitsanker / EF.C.TSL.CA\_2

* + 1. Genau wie EF.C.TSL.CA\_1 in Kapitel 5.7.2 enthält diese Datei ein Zertifikat mit dem öffentlichen Schlüssel PuK.TSL.CA\_2. Dieser öffentliche Schlüssel dient der Verifikation des Zertifikates C.TSL.SIG. Bei C.TSL.CA\_2 handelt es sich um ein CA-Zertifikat. Falls der Fehlbedienungszähler *retryCounter* von PIN.TSL\_CA\_2 den Wert null besitzt, dann sind weitere Änderungen des Dateiinhaltes unmöglich.
    2. **⌦ Card-G2-A\_2656 K\_Initialisierung: Initialisierte Attribute von MF / DF.Sicherheitsanker / EF.C.TSL.CA\_2**
* Das Objekt EF.C.TSL.CA\_2 MUSS die in Tab\_gSMC-K\_ObjSys\_078 dargestellten Werte besitzen.

Tabelle 130: Tab\_gSMC-K\_ObjSys\_078 Initialisierte Attribute von MF / DF.Sicherheitsanker / EF.C.TSL.CA\_2

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ‘C6 02’ |  |
| *shortFileIdentifier* | ‘02’ = 2 |  |
| *numberOfOctet* | ‘08 02’ Oktett = 2.050 Oktett |  |
| *positionLogicalEndOfFile* | ’0’ |  |
| *flagTransactionMode* | True |  |
| *flagChecksum* | False |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *shareable* | True |  |
| body | kein Inhalt |  |
| Zugriffsregel für logischen LCS „Operational state (activated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Read Binary | ALWAYS |  |
| Erase Binary  Set Logical EOF  Update Binary  Write Binary | PWD(PIN.TSL\_CA) |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (124) |
| Zugriffsregel für logischen LCS „Termination state“ | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (124) |

* + 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.Sicherheitsanker / PIN.BNetzA\_RCA

* + 1. Dieses Passwortobjekt wird zur Freischaltung des Kommandos UPDATE BINARY für die Datei EF.C.BNetzA.RCA (siehe Kapitel 5.7.1) verwendet.
    2. **⌦ Card-G2-A\_2658 K\_Initialisierung: Initialisierte Attribute von MF / DF.Sicherheitsanker / PIN.BNetzA\_RCA**
* Das Objekt PIN.BNetzA\_RCA MUSS die in Tab\_gSMC-K\_ObjSys\_080 dargestellten Werte besitzen.

Tabelle 131: Tab\_gSMC-K\_ObjSys\_080 Initialisierte Attribute von MF / DF.Sicherheitsanker / PIN.BNetzA\_RCA

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | Passwortobjekt |  |
| *pwdIdentifier* | ‘00’ = 0 |  |
| *secret* | undefiniert | wird personalisiert |
| *minimumLength* | 12 |  |
| *maximumLength* | 12 |  |
| *startRetryCounter* | 3 |  |
| *retryCounter* | 3 |  |
| *transportStatus* | ein Wert aus der Menge {Leer-PIN, Transport-PIN} |  |
| *flagEnabled* | True |  |
| *startSsec* | unendlich |  |
| *PUK* | kein Inhalt | keine PUK |
| *pukUsage* | 0 | keine PUK |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregel für logischen LCS „Operational state (activated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Change RD, P1=1 | ALWAYS | siehe Hinweis (129) |
| herstellerspezifisch | siehe [Card-G2-A\_2659] |
| Change RD, P1=0 | ALWAYS | siehe Hinweis (130) |
| Get Pin Status | ALWAYS |  |
| Verify | ALWAYS |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (124) |
| Zugriffsregel für logischen LCS „Termination state“ | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (124) |

* + 1. **⌫**

1. Kommandos, die gemäß [gemSpec\_COS] mit einem Passwortobjekt arbeiten, sind: Activate, Change Reference Data, Deactivate, Delete, Disable Verification Requirement, Enable Verification Requirement, Get Pin Status, Reset Retry Counter, Verify, Terminate
2. Diese Tabellenzeile gilt für den Fall transportStatus gleich Leer-PIN.
3. Diese Tabellenzeile gilt für den Fall transportStatus ungleich Leer-PIN.
   * 1. **⌦** **Card-G2-A\_2659 K\_Initialisierung: CHANGE REFERENCE DATA bei Nutzung der Leer-PIN für PIN.BNetzA\_RCA**

* Wenn für PIN.BnetzA\_RCA als Transportschutz Leer-PIN verwendet wird, dann DARF PIN.BnetzA\_RCA nicht personalisiert werden und es DARF im Zustand *transportStatus* gleich *regularPassword* das Attribut *secret* NICHT mit der Variante CHANGE REFERENCE DATA mit P1=1 änderbar sein. Die letzte Anforderung ist herstellerspezifisch umzusetzen.
  + 1. **⌫**
    2. **⌦ Card-G2-A\_3438 K\_Personalisierung: Personalisierte Attribute von MF / DF.Sicherheitsanker / PIN.BNetzA\_RCA**
* Wenn der Wert des Attributes transportStatus Transport–PIN ist, MÜSSEN bei der Personalisierung von PIN.BNetzA\_RCA die in Tab\_gSMC-K\_ObjSys\_146 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 132: Tab\_gSMC-K\_ObjSys\_146 Attribute von MF / DF.Sicherheitsanker / PIN.BNetzA\_RCA

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| secret | PIN-Wert gemäß [gemSpec\_PINPUK\_TI] | wird personalisiert |
| *transportStatus* | Transport-PIN | wird gegebenenfalls personalisiert, siehe Hinweis (131) |

* + 1. **⌫**

1. Für transportStatus wird der Wert „Transport-PIN“ initialisiert. Beispielsweise durch das Kommando Change Reference Data ist es möglich, diesen Wert im Rahmen der Personalisierung auf „regularPassword“ zu setzen.

### MF/DF.Sicherheitsanker / PIN.TSL\_CA

* + 1. Dieses Passwortobjekt wird zur Freischaltung des Kommandos UPDATE BINARY für die Datei EF.C.TSL.CA\_1 (siehe Kapitel 5.7.2) und EF.C.TSL.CA\_2 (siehe Kapitel 5.7.3) verwendet.
    2. **⌦ Card-G2-A\_2660 K\_Initialisierung: Initialisierte Attribute von MF / DF.Sicherheitsanker / PIN.TSL\_CA**
* Das Objekt PIN.TSL\_CA MUSS die in Tab\_gSMC-K\_ObjSys\_081 dargestellten Werte besitzen.

Tabelle 133: Tab\_gSMC-K\_ObjSys\_081 Initialisierte Attribute von MF / DF.Sicherheitsanker / PIN.TSL\_CA

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | Passwortobjekt |  |
| *pwdIdentifier* | ‘01’ = 1 |  |
| *secret* | undefiniert | wird personalisiert |
| *minimumLength* | 12 |  |
| *maximumLength* | 12 |  |
| *startRetryCounter* | 3 |  |
| *retryCounter* | 3 |  |
| *transportStatus* | ein Wert aus der Menge {Leer-PIN, Transport-PIN} |  |
| *flagEnabled* | True |  |
| *startSsec* | unendlich |  |
| *PUK* | kein Inhalt | keine PUK |
| *pukUsage* | 0 | keine PUK |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| Zugriffsregel für logischen LCS „Operational state (activated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Change RD, P1=1 | ALWAYS | siehe Hinweis (133) |
| herstellerspezifisch | siehe Hinweis (133) |
| Change RD, P1=0 | ALWAYS | siehe Hinweis (134) |
| Get Pin Status | ALWAYS |  |
| Verify | ALWAYS |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (124) |
| Zugriffsregel für logischen LCS „Termination state“ | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch | siehe Hinweis (124) |

* + 1. **⌫**

1. Kommandos, die gemäß [gemSpec\_COS]] mit einem Passwortobjekt arbeiten, sind: Activate, Change Reference Data, Deactivate, Delete, Disable Verification Requirement, Enable Verification Requirement, Get Pin Status, Reset Retry Counter, Verify, Terminate
2. Diese Tabellenzeile gilt für den Fall transportStatus gleich Leer-PIN.
3. Diese Tabellenzeile gilt für den Fall transportStatus ungleich Leer-PIN.
   * 1. **⌦ Card-G2-A\_2661 K\_Initialisierung: CHANGE REFERENCE DATA bei Nutzung der Leer-PIN für PIN.TSL\_CA**

* Wenn für PIN.TSL\_CA als Transportschutz Leer-PIN verwendet wird, dann DARF PIN.TSL\_CA nicht personalisiert werden und es DARF im Zustand *transportStatus* gleich *regularPassword* das Attribut *secret* NICHT mit der Variante CHANGE REFERENCE DATA mit P1=1 änderbar sein. Die letzte Anforderung ist herstellerspezifisch umzusetzen.
  + 1. **⌫**
    2. **⌦ Card-G2-A\_3439 K\_Personalisierung: Personalisierte Attribute von MF / DF.Sicherheitsanker / PIN.TSL\_CA**
* Wenn der Wert des Attributes transportStatus ransport–PIN ist, MÜSSEN bei der Personalisierung von PIN.TSL\_CA die in Tab\_gSMC-K\_ObjSys\_147 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 134: Tab\_gSMC-K\_ObjSys\_147 Attribute von MF / DF.Sicherheitsanker / PIN.TSL\_CA

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| secret | PIN-Wert gemäß [gemSpec\_PINPUK\_TI] | wird personalisiert |
| *transportStatus* | Transport-PIN | wird gegebenenfalls personalisiert, siehe Hinweis (135) |

* + 1. **⌫**

1. Für transportStatus wird der Wert „Transport-PIN“ initialisiert. Beispielsweise durch das Kommando Change Reference Data ist es möglich, diesen Wert im Rahmen der Personalisierung auf „regularPassword“ zu setzen.

## Zusätzliche Applikationen und Dateien

* + 1. Da eine gSMC-K innerhalb der TI nicht als eigenständige Komponente verwendet wird, sondern lediglich als Teilkomponente innerhalb eines Konnektors, ist es möglich, dass ein bestimmter Konnektor für den Betrieb weitere Objekte auf einer gSMC-K erwartet. Die Anforderungen in diesem Kapitel sind dazu gedacht, einem Konnektorhersteller in gewissem Rahmen eine Planungssicherheit zu geben, was die Installation weiterer Applikationen und Dateien anbelangt.
    2. **⌦** **Card-G2-A\_2662 K\_Initialisierung: Zahl der Ordner in MF, DF.AK, DF.NK, DF.SAK, DF.Sicherheitsanker**
* Für jeden Ordner, sofern vorhanden, aus der Menge {MF, DF.AK, DF.NK, DF.SAK, DF.Sicherheitsanker} gilt:

1. Es MUSS möglich sein, im Ordner bis zu vier Dateien anzulegen.
2. Für jede Datei gilt:
   1. Es MUSS möglich sein, dass die Datei durch bis zu zwei individuelle Zugriffsregel geschützt wird.
   2. Jede dieser Zugriffsregeln MUSS gemäß [gemSpec\_COS] kodierbar sein und MUSS insbesondere den Punkt [gemSpec\_COS#N007.170] beachten.
   3. Die Zugriffsregeln einer Datei DÜRFEN bei einer Kodierung gemäß [ISO7816-4] Kapitel 5.4.3.2 zusammen NICHT mehr als 128 Oktette beanspruchen.
      1. **⌫**
      2. **⌦** **Card-G2-A\_2663 K\_gSMC-K: Anlegen von EF.GeneralPurpose in MF, DF.AK, DF.NK, DF.SAK, DF.Sicherheitsanker**

* Es MUSS möglich sein

1. in mindestens einem Ordner aus der Menge {MF, DF.AK, DF.NK, DF.SAK, DF.Sicherheitsanker}, sofern dieser vorhanden ist
2. die in Tab\_gSMC-K\_ObjSys\_082 spezifizierte Datei anzulegen.
   * 1. **⌫**
3. Card-G2-A\_2662 stellt sicher, dass für die Zugriffsregeln immer eine gewisse Menge an Speicherplatz vorhanden ist. Das gilt z.B. auch, wenn das COS die Zugriffregeln analog zu [ISO7816-4] Kapitel 5.4.3.3 in einem EF.ARR speichert.
4. Card-G2-A\_2663 stellt sicher, dass eine gewisse Menge an freiem Speicherplatz zur Verfügung steht. Dabei fordert Card-G2-A\_2663 a, dass in jedem vorhandenen Ordner der hier geforderte Speicherplatz auch exklusiv zur Verfügung steht. Demgegenüber stellt Card-G2-A\_2663 b eine Forderung nach der Mindestmenge an gesamten freien Speicher dar.

## EF.GeneralPurpose (kann nach Ausgabe der gSMC-K nachgeladen werden)

* + 1. **⌦ Card-G2-A\_2664 Attribute der nachladbaren Datei EF.GeneralPurpose**
* Falls das Objekt EF.GeneralPurpose auf die gSMC-K nachgeladen wird, MUSS es die in Tab\_gSMC-K\_ObjSys\_082 dargestellten Werte besitzen.

Tabelle 135: Tab\_gSMC-K\_ObjSys\_082 Attribute der nachladbaren Datei EF.GeneralPurpose

|  |  |  |
| --- | --- | --- |
| Attribute | Wert | Bemerkung |
| Objekttyp | transparentes Elementary File |  |
| *fileIdentifier* | ‘10 00’ |  |
| *shortFileIdentifier* | – |  |
| *numberOfOctet* | ‘2000’ Oktett = 8.192 Oktett |  |
| *positionLogicalEndOfFile* | Zahl der tatsächlich belegten Oktette |  |
| *flagTransactionMode* | True |  |
| *flagChecksum* | False |  |
| *lifeCycleStatus* | „Operational state (activated)“ |  |
| *shareable* | True |  |
| *body* | ‘XX…YY’ |  |
| Zugriffsregel für logischen LCS „Operational state (activated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| Delete | ALWAYS |  |
| Read Binary | ALWAYS |  |
| Erase Binary  Set Logical EOF  Update Binary  Write Binary | ALWAYS |  |
| andere | NEVER |  |
| Zugriffsregel für logischen LCS „Operational state (deactivated)” | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |
| Zugriffsregel für logischen LCS „Termination state“ | | |
| Zugriffsart | Zugriffsbedingung | Bemerkung |
| alle | herstellerspezifisch |  |

* + 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.

## Laden einer neuen Anwendung oder Anlegen eines EFs oder Sperren von Schlüsseln nach Ausgabe der gSMC-K

* + 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.Version) nach der Ausgabe der gSMC-K von einem Card Management System (CMS) durchgeführt wird. Dies ist ein optionaler Prozess.
    2. Ebenso ist das CMS optional. Die Inhalte des Kapitels 14 in [gemSpec\_COS] sind allerdings normativ, wenn das Laden neuer Anwendungen oder das Erstellen neuer EFs nach Aus¬gabe der gSMC-K durchgeführt werden.

# 

# Anhang A - Verzeichnisse

## A1 – Abkürzungen

|  |  |
| --- | --- |
| **Kürzel** | **Erläuterung** |
| AK | Anwendungskonnektor |
| APDU | Application Protocol Data Unit |
| ATR | Answer to Reset |
| CA | Certification Authority |
| CHAT | Certificate Holder Autorisation Template Liste von Rechten, die ein Zertifikatsinhaber besitzt |
| CMS | Card Management System |
| COS | Card Operating System, Kartenbetriebssystem |
| CUP | Certificate Update |
| C2C | Card to Card |
| DF | Dedicated File |
| EF | Elementary File |
| ELC | Elliptic Curve Cryptography, Kryptographie mittels elliptischer Kurven |
| GDO | Global Data Object |
| HBA | Heilberufeausweis |
| MF | Master File |
| NK | Netzkonnektor |
| RCA | Root Certification Authority |
| SAK | Signaturanwendungskomponente |
| TPM | Trusted Platform Module |
| TSL | Trust-service Status List |
| VPN | Virtual Private Network |

## A2 – Glossar

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

## A3 – Abbildungsverzeichnis

[Abbildung 1: Abb\_gSMC-K\_ObjSys\_001 Dateistruktur einer gSMC-K auf oberster Ebene 22](#_Toc465424772)

[Abbildung 2: Abb\_gSMC-K\_ObjSys\_002 Dateistruktur der Anwendung DF.AK 80](#_Toc465424773)

[Abbildung 3: Abb\_gSMC-K\_ObjSys\_003 Dateistruktur der Anwendung DF.NK 93](#_Toc465424774)

[Abbildung 4: Abb\_gSMC-K\_ObjSys\_004 Objektstruktur der Anwendung DF.SAK 111](#_Toc465424775)

[Abbildung 5: Abb\_gSMC-K\_ObjSys\_005 Dateistruktur der Anwendung DF.Sicherheitsanker 132](#_Toc465424776)

## A4 – Tabellenverzeichnis

[Tabelle 1: Tab\_gSMC-K\_ObjSys\_001 Liste der Komponenten, aus deren Sicht Anforderungen betrachtet werden 11](#_Toc465424780)

[Tabelle 2: Tab\_gSMC-K\_ObjSys\_002 ATR-Kodierung 20](#_Toc465424781)

[Tabelle 3: Tab\_gSMC-K\_ObjSys\_004 - Initialisierte Attribute von MF 23](#_Toc465424782)

[Tabelle 4: Tab\_gSMC-K\_ObjSys\_005 - Initialisierte Attribute von MF / EF.ATR 23](#_Toc465424783)

[Tabelle 5: Tab\_gSMC-K\_ObjSys\_009 Initialisierte Attribute von MF / EF.DIR 24](#_Toc465424784)

[Tabelle 6: Tab\_gSMC-K\_ObjSys\_010 Initialisierte Attribute von MF / EF.EnvironmentSettings 26](#_Toc465424785)

[Tabelle 7: Tab\_gSMC-K\_ObjSys\_090 Attribute von MF / EF.EnvironmentSettings 26](#_Toc465424786)

[Tabelle 8: Tab\_gSMC-K\_ObjSys\_011 Initialisierte Attribute von MF / EF.GDO 27](#_Toc465424787)

[Tabelle 9: Tab\_gSMC-K\_ObjSys\_177 Personalisierte Attribute von MF / EF.GDO 28](#_Toc465424788)

[Tabelle 10: Tab\_ gSMC-K\_ObjSys\_150 Initialisierte Attribute von MF / EF.KeyInfo 28](#_Toc465424789)

[Tabelle 11 Tab\_gSMC-K\_ObjSys\_012 Initialisierte Attribute von MF / EF.Version2 29](#_Toc465424790)

[Tabelle 12: Tab\_gSMC-K\_ObjSys\_007 Initialisierte Attribute von MF / EF.C.CA\_SAK.CS.E256 30](#_Toc465424791)

[Tabelle 13: Tab\_gSMC-K\_ObjSys\_087 Attribute von MF / EF.C.CA\_SAK.CS.E256 31](#_Toc465424792)

[Tabelle 14: Tab\_gSMC-K\_ObjSys\_008 Initialisierte Attribute von MF / EF.C.CA\_SAK.CS.E384 32](#_Toc465424793)

[Tabelle 15: Tab\_gSMC-K\_ObjSys\_176 Initialisierte Attribute von MF / EF.PuK.RCA.CS.R2048 32](#_Toc465424794)

[Tabelle 16:Tab\_gSMC-K\_ObjSys\_148 Personalisierte Attribute von MF / EF.PuK.RCA.CS.R2048 für Testkarten 33](#_Toc465424795)

[Tabelle 17: Tab\_gSMC-K\_ObjSys\_084 Initialisierte Attribute von MF / EF.C.RCA.CS.E256 34](#_Toc465424796)

[Tabelle 18:Tab\_gSMC-K\_ObjSys\_149 Personalisierte Attribute von MF / EF.C.RCA.CS.E256 für Testkarten 35](#_Toc465424797)

[Tabelle 19: Tab\_gSMC-K\_ObjSys\_192 Initialisierte Attribute von MF / EF.C.SMC.AUT\_CVC.E256 35](#_Toc465424798)

[Tabelle 20: Tab\_gSMC-K\_ObjSys\_193 Personalisierte Attribute von MF / EF.C.SMC.AUT\_CVC.E256 36](#_Toc465424799)

[Tabelle 21: Tab\_gSMC-K\_ObjSys\_194 Initialisierte Attribute von MF / EF.C.SMC.AUT\_CVC.E384 37](#_Toc465424800)

[Tabelle 22: Tab\_gSMC-K\_ObjSys\_013 Initialisierte Attribute von MF / PIN.AK 38](#_Toc465424801)

[Tabelle 23: Tab\_gSMC-K\_ObjSys\_094 Attribute von MF / PIN.AK 39](#_Toc465424802)

[Tabelle 24: Tab\_gSMC-K\_ObjSys\_014 Initialisierte Attribute von MF / PIN.NK 39](#_Toc465424803)

[Tabelle 25: Tab\_gSMC-K\_ObjSys\_095 Attribute von MF / PIN.NK 41](#_Toc465424804)

[Tabelle 26: Tab\_gSMC-K\_ObjSys\_015 Initialisierte Attribute von MF / PIN.Pers 41](#_Toc465424805)

[Tabelle 27: Tab\_gSMC-K\_ObjSys\_096 Attribute von MF / PIN.Pers 42](#_Toc465424806)

[Tabelle 28: Tab\_gSMC-K\_ObjSys\_016 Initialisierte Attribute von MF / PIN.SAK 43](#_Toc465424807)

[Tabelle 29: Tab\_gSMC-K\_ObjSys\_097 Attribute von MF / PIN.SAK 44](#_Toc465424808)

[Tabelle 30: Tab\_gSMC-K\_ObjSys\_195 Initialisierte Attribute von MF / PrK.SMC.AUT\_CVC.E256 44](#_Toc465424809)

[Tabelle 31: Tab\_gSMC-K\_ObjSys\_196 Personalisierte Attribute von MF / PrK.SMC.AUT\_CVC.E256 46](#_Toc465424810)

[Tabelle 32: Tab\_gSMC-K\_ObjSys\_197 Initialisierte Attribute von MF / PrK.SMC.AUT\_CVC.E384 46](#_Toc465424811)

[Tabelle 33: Tab\_gSMC-K\_ObjSys\_017 Initialisierte Attribute von MF / PrK.KONN.AUT.R2048 48](#_Toc465424812)

[Tabelle 34: Tab\_gSMC-K\_ObjSys\_098 Attribute von MF / PrK.KONN.AUT.R2048 49](#_Toc465424813)

[Tabelle 35: Tab\_gSMC-K\_ObjSys\_152 Initialisierte Attribute von MF / PrK.KONN.AUT2.R2048 49](#_Toc465424814)

[Tabelle 36: Tab\_gSMC-K\_ObjSys\_018 Initialisierte Attribute von MF / PrK.KONN.AUT.R3072 50](#_Toc465424815)

[Tabelle 37: Tab\_gSMC-K\_ObjSys\_178 Initialisierte Attribute von MF / PrK.KONN.AUT.E256 51](#_Toc465424816)

[Tabelle 38: Tab\_gSMC-K\_ObjSys\_019 Initialisierte Attribute von MF / PrK.KONN.AUT.E384 52](#_Toc465424817)

[Tabelle 39: Tab\_gSMC-K\_ObjSys\_020 Initialisierte Attribute von MF / PrK.GP.R2048 64](#_Toc465424818)

[Tabelle 40: Tab\_gSMC-K\_ObjSys\_101 Attribute von MF / PrK.GP.R2048 65](#_Toc465424819)

[Tabelle 41: Tab\_gSMC-K\_ObjSys\_027 Initialisierte Attribute von MF / PuK.GP.R2048 66](#_Toc465424820)

[Tabelle 42: Tab\_gSMC-K\_ObjSys\_104 Attribute von MF / PuK.GP.R2048 66](#_Toc465424821)

[Tabelle 43: Tab\_gSMC-K\_ObjSys\_153 Initialisierte Attribute von MF / PrK.GP2.R2048 67](#_Toc465424822)

[Tabelle 44: Tab\_gSMC-K\_ObjSys\_021 Initialisierte Attribute von MF / PrK.GP.R3072 67](#_Toc465424823)

[Tabelle 45: Tab\_gSMC-K\_ObjSys\_179 Initialisierte Attribute von MF / PrK.GP.E256 68](#_Toc465424824)

[Tabelle 46: Tab\_gSMC-K\_ObjSys\_022 Initialisierte Attribute von MF / PrK.GP.E384 69](#_Toc465424825)

[Tabelle 47: Tab\_gSMC-K\_ObjSys\_024 Initialisierte Attribute von MF / PuK.RCA.CS.E256 70](#_Toc465424826)

[Tabelle 48: Tab\_gSMC-K\_ObjSys\_191 Personalisierte Attribute von MF / PuK.RCA.CS.E256 für Testkarten 71](#_Toc465424827)

[Tabelle 49: Tab\_gSMC-K\_ObjSys\_085 Initialisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256 72](#_Toc465424828)

[Tabelle 50: Tab\_gSMC-K\_ObjSys\_108 Attribute von MF / PuK.RCA.ADMINCMS.CS.E256 73](#_Toc465424829)

[Tabelle 51: Tab\_gSMC-K\_ObjSys\_030 Initialisierte Attribute von MF / SK.CMS.AES128 74](#_Toc465424830)

[Tabelle 52: Tab\_gSMC-K\_ObjSys\_110 Attribute von MF / SK.CMS.AES128 75](#_Toc465424831)

[Tabelle 53: Tab\_gSMC-K\_ObjSys\_031 Initialisierte Attribute von MF / SK.CMS.AES256 75](#_Toc465424832)

[Tabelle 54: Tab\_gSMC-K\_ObjSys\_111 Attribute von MF / SK.CMS.AES256 76](#_Toc465424833)

[Tabelle 55: Tab\_gSMC-K\_ObjSys\_154 Initialisierte Attribute von MF / SK.CUP.AES128 77](#_Toc465424834)

[Tabelle 56: Tab\_gSMC-K\_ObjSys\_155 Personalisierte Attribute von MF / SK.CUP.AES128 77](#_Toc465424835)

[Tabelle 57: Tab\_gSMC-K\_ObjSys\_156 Initialisierte Attribute von MF / SK.CUP.AES256 78](#_Toc465424836)

[Tabelle 58: Tab\_gSMC-K\_ObjSys\_157 Personalisierte Attribute von MF / SK.CUP.AES256 78](#_Toc465424837)

[Tabelle 59: Tab\_gSMC-K\_ObjSys\_032 Initialisierte Attribute von MF / DF.AK 79](#_Toc465424838)

[Tabelle 60: Tab\_gSMC-K\_ObjSys\_034 Initialisierte Attribute von MF / DF.AK / EF.C.AK.AUT.R2048 80](#_Toc465424839)

[Tabelle 61: Tab\_gSMC-K\_ObjSys\_158 Attribute von MF / DF.AK / EF.C.AK.AUT.R2048 81](#_Toc465424840)

[Tabelle 62: Tab\_gSMC-K\_ObjSys\_036 Initialisierte Attribute von MF / DF.AK / PrK.AK.AUT.R2048 82](#_Toc465424841)

[Tabelle 63: Tab\_gSMC-K\_ObjSys\_113 Attribute von MF / DF.AK / PrK.AK.AUT.R2048 83](#_Toc465424842)

[Tabelle 64: Tab\_gSMC-K\_ObjSys\_159 Initialisierte Attribute von MF / DF.AK / EF.C.AK.AUT2.XXXX 83](#_Toc465424843)

[Tabelle 65: Tab\_gSMC-K\_ObjSys\_187 Initialisierte Attribute von MF / DF.AK / PrK.AK.AUT2.R2048 85](#_Toc465424844)

[Tabelle 66: Tab\_gSMC-K\_ObjSys\_160 Initialisierte Attribute von MF / DF.AK / PrK.AK.AUT.R3072 85](#_Toc465424845)

[Tabelle 67: Tab\_gSMC-K\_ObjSys\_161 Initialisierte Attribute von MF / DF.AK / PrK.AK.AUT.E256 86](#_Toc465424846)

[Tabelle 68: Tab\_gSMC-K\_ObjSys\_162 Initialisierte Attribute von MF / DF.AK / PrK.AK.AUT.E384 87](#_Toc465424847)

[Tabelle 69: Tab\_gSMC-K\_ObjSys\_037 Initialisierte Attribute von MF / DF.AK / PrK.AK.CA\_PS.R2048 88](#_Toc465424848)

[Tabelle 70: Tab\_gSMC-K\_ObjSys\_114 Attribute von MF / DF.AK / PrK.AK.CA\_PS.R2048 89](#_Toc465424849)

[Tabelle 71: Tab\_gSMC-K\_ObjSys\_180 Initialisierte Attribute von MF / DF.AK / PrK.AK.CA\_PS2.R2048 89](#_Toc465424850)

[Tabelle 72: Tab\_gSMC-K\_ObjSys\_038 Initialisierte Attribute von MF / DF.AK / PrK.AK.CA\_PS.R3072 90](#_Toc465424851)

[Tabelle 73: Tab\_gSMC-K\_ObjSys\_181 Initialisierte Attribute von MF / DF.AK / PrK.AK.CA\_PS.E256 90](#_Toc465424852)

[Tabelle 74: Tab\_gSMC-K\_ObjSys\_039 Initialisierte Attribute von MF / DF.AK / PrK.AK.CA\_PS.E384 91](#_Toc465424853)

[Tabelle 75: Tab\_gSMC-K\_ObjSys\_040 Initialisierte Attribute von MF / DF.NK 92](#_Toc465424854)

[Tabelle 76: Tab\_gSMC-K\_ObjSys\_041 Initialisierte Attribute von MF / DF.NK / EF.ActKey 93](#_Toc465424855)

[Tabelle 77: Tab\_gSMC-K\_ObjSys\_042 Initialisierte Attribute von MF / DF.NK / EF.CardInfo 94](#_Toc465424856)

[Tabelle 78: Tab\_gSMC-K\_ObjSys\_043 Initialisierte Attribute von MF / DF.NK / EF.CFSMACKey 95](#_Toc465424857)

[Tabelle 79: Tab\_gSMC-K\_ObjSys\_044 Initialisierte Attribute von MF / DF.NK / EF.ConfigUser 96](#_Toc465424858)

[Tabelle 80: Tab\_gSMC-K\_ObjSys\_046 Initialisierte Attribute von MF / DF.NK / EF.C.NK.VPN.R2048 97](#_Toc465424859)

[Tabelle 81: Tab\_gSMC-K\_ObjSys\_121 Attribute von MF / DF.NK / EF.C.NK.VPN.R2048 98](#_Toc465424860)

[Tabelle 82: Tab\_gSMC-K\_ObjSys\_188 Initialisierte Attribute von MF / DF.NK / PrK.NK.VPN.R2048 98](#_Toc465424861)

[Tabelle 83: Tab\_gSMC-K\_ObjSys\_163 Attribute von MF / DF.NK / PrK.NK.VPN.R2048 99](#_Toc465424862)

[Tabelle 84: Tab\_gSMC-K\_ObjSys\_189 Initialisierte Attribute von MF / DF.NK / EF.C.NK.VPN2.XXXX 100](#_Toc465424863)

[Tabelle 85: Tab\_gSMC-K\_ObjSys\_164 Initialisierte Attribute von MF / DF.NK / PrK.NK.VPN2.R2048 101](#_Toc465424864)

[Tabelle 86: Tab\_gSMC-K\_ObjSys\_190 Initialisierte Attribute von MF / DF.NK / PrK.NK.VPN.R3072 102](#_Toc465424865)

[Tabelle 87: Tab\_gSMC-K\_ObjSys\_165 Initialisierte Attribute von MF / DF.NK / PrK.NK.VPN.E256 102](#_Toc465424866)

[Tabelle 88: Tab\_gSMC-K\_ObjSys\_166 Initialisierte Attribute von MF / DF.NK / PrK.NK.VPN.E384 103](#_Toc465424867)

[Tabelle 89: Tab\_gSMC-K\_ObjSys\_049 Initialisierte Attribute von MF / DF.NK / PrK.CFS.R2048 104](#_Toc465424868)

[Tabelle 90: Tab\_gSMC-K\_ObjSys\_123 Attribute von MF / DF.NK / PrK.CFS.R2048 105](#_Toc465424869)

[Tabelle 91: Tab\_gSMC-K\_ObjSys\_055 Initialisierte Attribute von MF / DF.NK / PuK.CFS.R2048 105](#_Toc465424870)

[Tabelle 92: Tab\_gSMC-K\_ObjSys\_130 Attribute von MF / DF.NK / PuK.CFS.R2048 106](#_Toc465424871)

[Tabelle 93: Tab\_gSMC-K\_ObjSys\_182 Initialisierte Attribute von MF / DF.NK / PrK.CFS2.R2048 106](#_Toc465424872)

[Tabelle 94: Tab\_gSMC-K\_ObjSys\_050 Initialisierte Attribute von MF / DF.NK / PrK.CFS.R3072 107](#_Toc465424873)

[Tabelle 95: Tab\_gSMC-K\_ObjSys\_183 Initialisierte Attribute von MF / DF.NK / PrK.CFS.E256 108](#_Toc465424874)

[Tabelle 96: Tab\_gSMC-K\_ObjSys\_051 Initialisierte Attribute von MF / DF.NK / PrK.CFS.E384 109](#_Toc465424875)

[Tabelle 97: Tab\_gSMC-K\_ObjSys\_058 Initialisierte Attribute von MF / DF.SAK 110](#_Toc465424876)

[Tabelle 98: Tab\_gSMC-K\_ObjSys\_167 Initialisierte Attribute von MF / DF.SAK / EF.C.SAK.AUT.R2048 111](#_Toc465424877)

[Tabelle 99: Tab\_gSMC-K\_ObjSys\_133 Attribute von MF / DF.SAK / EF.C.SAK.AUT.R2048 112](#_Toc465424878)

[Tabelle 100: Tab\_gSMC-K\_ObjSys\_168 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUT.R2048 113](#_Toc465424879)

[Tabelle 101: Tab\_gSMC-K\_ObjSys\_169 Attribute von MF / DF.SAK / PrK.SAK.AUT.R2048 114](#_Toc465424880)

[Tabelle 102: Tab\_gSMC-K\_ObjSys\_060 Initialisierte Attribute von MF / DF.SAK / EF.C.SAK.AUT2.XXXX 114](#_Toc465424881)

[Tabelle 103: Tab\_gSMC-K\_ObjSys\_170 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUT2.R2048 115](#_Toc465424882)

[Tabelle 104: Tab\_gSMC-K\_ObjSys\_171 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUT.R3072 116](#_Toc465424883)

[Tabelle 105: Tab\_gSMC-K\_ObjSys\_172 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUT.E256 117](#_Toc465424884)

[Tabelle 106: Tab\_gSMC-K\_ObjSys\_173 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUT.E384 117](#_Toc465424885)

[Tabelle 107: Tab\_gSMC-K\_ObjSys\_064 Initialisierte Attribute von MF / DF.SAK / EF.C.SAK.AUTD\_CVC.E256 118](#_Toc465424886)

[Tabelle 108: Tab\_gSMC-K\_ObjSys\_135 Attribute von MF / DF.SAK / EF.C.SAK.AUTD\_CVC.E256 119](#_Toc465424887)

[Tabelle 109: Tab\_gSMC-K\_ObjSys\_067 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUTD\_CVC.E256 119](#_Toc465424888)

[Tabelle 110: Tab\_gSMC-K\_ObjSys\_137 Attribute von MF / DF.SAK / PrK.SAK.AUTD\_CVC.E256 120](#_Toc465424889)

[Tabelle 111: Tab\_gSMC-K\_ObjSys\_065 Initialisierte Attribute von MF / DF.SAK / EF.C.SAK.AUTD\_CVC.E384 121](#_Toc465424890)

[Tabelle 112: Tab\_gSMC-K\_ObjSys\_068 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUTD\_CVC.E384 122](#_Toc465424891)

[Tabelle 113: Tab\_gSMC-K\_ObjSys\_069 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.CA\_xTV.R2048 122](#_Toc465424892)

[Tabelle 114: Tab\_gSMC-K\_ObjSys\_139 Attribute von MF / DF.SAK / PrK.SAK.CA\_xTV.R2048 123](#_Toc465424893)

[Tabelle 115: Tab\_gSMC-K\_ObjSys\_174 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.CA\_xTV2.R2048 124](#_Toc465424894)

[Tabelle 116: Tab\_gSMC-K\_ObjSys\_070 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.CA\_xTV.R3072 124](#_Toc465424895)

[Tabelle 117: Tab\_gSMC-K\_ObjSys\_184 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.CA\_xTV.E256 125](#_Toc465424896)

[Tabelle 118: Tab\_gSMC-K\_ObjSys\_071 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.CA\_xTV.E384 126](#_Toc465424897)

[Tabelle 119: Tab\_gSMC-K\_ObjSys\_072 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.SIG.R2048 127](#_Toc465424898)

[Tabelle 120: Tab\_gSMC-K\_ObjSys\_142 Attribute von MF / DF.SAK / PrK.SAK.SIG.R2048 128](#_Toc465424899)

[Tabelle 121: Tab\_gSMC-K\_ObjSys\_185 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.SIG2.R2048 128](#_Toc465424900)

[Tabelle 122: Tab\_gSMC-K\_ObjSys\_073 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.SIG.R3072 129](#_Toc465424901)

[Tabelle 123: Tab\_gSMC-K\_ObjSys\_186 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.SIG.E256 129](#_Toc465424902)

[Tabelle 124: Tab\_gSMC-K\_ObjSys\_074 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.SIG.E384 130](#_Toc465424903)

[Tabelle 125: Tab\_gSMC-K\_ObjSys\_075 Initialisierte Attribute von MF / DF.Sicherheitsanker 131](#_Toc465424904)

[Tabelle 126: Tab\_gSMC-K\_ObjSys\_076 Initialisierte Attribute von MF / DF.Sicherheitsanker / EF.C.BNetzA.RCA 132](#_Toc465424905)

[Tabelle 127: Tab\_gSMC-K\_ObjSys\_214 Personalisierte Attribute von MF / EF.C.BNetzA.RCA für Testkarten 133](#_Toc465424906)

[Tabelle 128: Tab\_gSMC-K\_ObjSys\_077 Initialisierte Attribute von MF / DF.Sicherheitsanker / EF.C.TSL.CA\_1 134](#_Toc465424907)

[Tabelle 129: Tab\_gSMC-K\_ObjSys\_215 Personalisierte Attribute von MF / EF.C.TSL.CA\_1 für Testkarten 135](#_Toc465424908)

[Tabelle 130: Tab\_gSMC-K\_ObjSys\_078 Initialisierte Attribute von MF / DF.Sicherheitsanker / EF.C.TSL.CA\_2 135](#_Toc465424909)

[Tabelle 131: Tab\_gSMC-K\_ObjSys\_080 Initialisierte Attribute von MF / DF.Sicherheitsanker / PIN.BNetzA\_RCA 136](#_Toc465424910)

[Tabelle 132: Tab\_gSMC-K\_ObjSys\_146 Attribute von MF / DF.Sicherheitsanker / PIN.BNetzA\_RCA 137](#_Toc465424911)

[Tabelle 133: Tab\_gSMC-K\_ObjSys\_081 Initialisierte Attribute von MF / DF.Sicherheitsanker / PIN.TSL\_CA 138](#_Toc465424912)

[Tabelle 134: Tab\_gSMC-K\_ObjSys\_147 Attribute von MF / DF.Sicherheitsanker / PIN.TSL\_CA 139](#_Toc465424913)

[Tabelle 135: Tab\_gSMC-K\_ObjSys\_082 Attribute der nachladbaren Datei EF.GeneralPurpose 140](#_Toc465424914)

## 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 des Card Operating System (COS) -  Elektrische Schnittstelle |
| [gemSpec\_Karten\_Fach\_TIP] | gematik: Befüllvorschriften für die Plattformanteile der Karten der TI |
|  |  |
| [gemSpec\_PINPUK\_TI] | gematik: Übergreifende Spezifikation PIN/PUK-Policy für Smartcards der Telematikinfrastruktur |
| [gemSpec\_OID] | gematik: Spezifikation Festlegung von OIDs |
| [gemSpec\_PKI] | gematik: Übergreifende Spezifikation Spezifikation PKI |
| [gemSpec\_Krypt] | gematik: Übergreifende Spezifikation - Verwendung krypto­graphischer Algorithmen in der Telematikinfrastruktur |
| [gemSpec\_CVC\_Root] | gematik: Spezifikation CVC - Root |
| [gemSpec\_CVC\_TSP] | gematik: Spezifikation Trust Service Provider CVC |
| [gemSpec\_TK] | gematik: Spezifikation für Testkarten gematik (eGK, HBA, (g)SMC) der Generation 2 |
| [gemSpec\_SMC\_OPT] | gematik: Spezifikation der Security Module Card (SMC) –  Gemeinsame optische Merkmale |

### A5.2 – Weitere Dokumente

| **[Quelle]** | **Herausgeber (Erscheinungsdatum): Titel** |
| --- | --- |
| [Beschluss 190] | Beschluss Nr. 190 der Europäischen Union vom 18. Juni 2003 betreffend die technischen Merkmale der europäischen Krankenversicherungskarte |
| [DIN\_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 |
| [ISO3166-1] | ISO/IEC 3166-1: Codes for the representations of names of countries |
| [ISO7816-3] | ISO/IEC 7816-3: Smart Card Standard:  Part 3: Electronic Signals and Transmission Protocols |
| [ISO7816-4] | 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) |
| [SD5] | ISO/IEC JTC1/SC17 STANDING DOCUMENT 5, 2006-06-19  Register of IC manufacturers |
| [PKCS#1v2.1] | PKCS #1 v2.1: RSA Cryptography Standard, RSA Laboratories, 2002-06-14 |
| [RFC2119] | RFC 2119 (März 1997): Key words for use in RFCs to Indicate Requirement Levels S. Bradner, <http://www.ietf.org/rfc/rfc2119.txt> |
| [TLS] | The Transport Layer Security (TLS) Protocol, Version 1.1, RFC 4346 |