

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation des elektronischen Heilberufsausweises HBA-Objektsystem

Version: [4.65.0.0 CC](#)
Revision: [241924266704](#)
Stand: [30.0605.08.2020](#)
Status: [zur Abstimmung](#) freigegeben
Klassifizierung: Öffentlich [Entwurf](#)
Referenzierung: gemSpec_HBA_ObjSys_G2.1

Dokumentinformationen

Änderungen zur Vorversion

Anpassungen des vorliegenden Dokumentes im Vergleich zur Vorversion können Sie der nachfolgenden Tabelle entnehmen.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
4.0.0	21.04.17		Einarbeitung Anpassungen Kartengeneration G2.1	gematik
4.1.0	18.12.17		Einarbeitung Errata R1.6.4-2	gematik
4.2.0	14.05.18		Anpassung auf Grundlage von P 15.2 und P 15.3	gematik
4.3.0	26.10.18		Einarbeitung P15.9	gematik
4.4.0	28.11.18		Einarbeitung P15.11	gematik
4.5.0	15.05.19		Einarbeitung P18.1	gematik
4.6.0	30.06.20		Anpassungen bzgl. kontaktloser Schnittstelle	gematik
5.0.0 CC	31.07.20		Anpassungen gemäß C 10271	gematik / afi

Inhaltsverzeichnis

1 Einordnung des Dokumentes	9
1.1 Zielsetzung	9
1.2 Zielgruppe	9
1.3 Geltungsbereich	10
1.4 Abgrenzung des Dokuments	10
1.5 Methodik	10
1.5.1 Nomenklatur	10
1.5.2 Verwendung von Schlüsselworten	13
1.5.3 Komponentenspezifische Anforderungen	13
2 Optionen	14
2.1 Option_Erstellung_von_Testkarten	14
3 Lebenszyklus von Karte und Applikation	15
4 Anwendungsübergreifende Festlegungen	16
4.1 Mindestanzahl logischer Kanäle	16
4.2 Unterstützung RSA CV Zertifikate	16
4.3 Unterstützung Onboard RSA Schlüsselgenerierung	16
4.4 Unterstützung optionaler Funktionspakete	16
4.4.1 USB Schnittstelle (optional)	16
4.4.2 Kontaktlose Schnittstelle (optional)	17
4.4.3 Kryptobox (optional)	18
4.4.4 Symmetrischer Kryptographicalgorithmus DES (optional)	18
4.5 Attributstabellen	19
4.5.1 Attribute eines Ordners	19
4.5.2 Attribute einer Datei (EF)	20
4.6 Zugriffsregeln für besondere Kommandos	20
4.7 Attributswerte und Personalisierung	21
4.8 Kartenadministration	22
5 Spezifikation grundlegender Applikationen	23
5.1 Attribute des Objektsystems	23
5.1.1 ATR Kodierung	24
5.2 Allgemeine Struktur	25
5.3 Root, die Wurzelapplikation MF	25
5.3.1 MF / EF.ATR	27
5.3.2 MF / EF.CardAccess (Option kontaktlose Schnittstelle)	29
5.3.3 MF / EF.DIR	30
5.3.4 MF / EF.GDO	33

65	5.3.5 MF / EF.Version2	35
66	5.3.6 MF / EF.C.CA_HPC.CS.E256	37
67	5.3.7 MF / EF.C.HPC.AUTR_CVC.E256	39
68	5.3.8 MF / EF.C.HPC.AUTD_SUK_CVC.E256	41
69	5.3.9 MF / PIN.CH	44
70	5.3.10 MF / PrK.HPC.AUTR_CVC.E256	46
71	5.3.11 MF / PrK.HPC.AUTD_SUK_CVC.E256	48
72	5.3.12 Sicherheitsanker zum Import von CV-Zertifikaten	51
73	5.3.12.1 MF / PuK.RCA.CS.E256	51
74	5.3.13 Asymmetrische Kartenadministration	54
75	5.3.13.1 MF / PuK.RCA.ADMINCMS.CS.E256	54
76	5.3.14 Symmetrische Kartenadministration	57
77	5.3.14.1 MF / SK.CMS.AES128	58
78	5.3.14.2 MF / SK.CMS.AES256	60
79	5.3.14.3 MF / SK.CUP.AES128	62
80	5.3.14.4 MF / SK.CUP.AES256	64
81	5.3.15 MF / SK.CAN (Option kontaktlose Schnittstelle)	66
82	5.3.16 Sicherheitsumgebungen auf MF-Ebene	68
83	5.4 Die Heilberufsanwendung DF.HPA	68
84	5.4.1 Dateistruktur und Dateiinhalt	68
85	5.4.2 MF / DF.HPA (Health Professional Application)	68
86	5.4.2.1 MF / DF.HPA / EF.HPD (Health Professional Data)	70
87	5.4.2.2 Sicherheitsumgebungen	71
88	5.5 Die Anwendung für die qualifizierte elektronische Signatur (DF.QES)	72
89	5.5.1 Dateistruktur und Dateiinhalt	72
90	5.5.2 MF / DF.QES (Qualified Electronic Signature Application)	72
91	5.5.2.1 MF / DF.QES / PrK.HP.QES.R2048	74
92	5.5.2.2 MF / DF.QES / PIN.QES	76
93	5.5.2.3 MF / DF.QES / EF.SSEC	79
94	5.5.2.4 MF / DF.QES / EF.C.HP.QES.R2048	82
95	5.5.2.5 MF / DF.QES / PrK.HP.QES.E256	84
96	5.5.2.6 MF / DF.QES / EF.C.HP.QES.E256	87
97	5.6 Die E-SIGN-Anwendung (DF.ESIGN)	89
98	5.6.1 Dateistruktur und Dateiinhalt	89
99	5.6.2 MF / DF.ESIGN (Krypto-Anwendung E-SIGN)	90
100	5.6.2.1 MF / DF.ESIGN / PrK.HP.AUT.R2048	91
101	5.6.2.2 MF / DF.ESIGN / PrK.HP.ENC.R2048	93
102	5.6.2.3 MF / DF.ESIGN / EF.C.HP.AUT.R2048	96
103	5.6.2.4 MF / DF.ESIGN / EF.C.HP.ENC.R2048	98
104	5.6.2.5 MF / DF.ESIGN / PrK.HP.AUT.E256	100
105	5.6.2.6 MF / DF.ESIGN / PrK.HP.ENC.E256	102
106	5.6.2.7 MF / DF.ESIGN / EF.C.HP.AUT.E256	105
107	5.6.2.8 MF / DF.ESIGN / EF.C.HP.ENC.E256	107
108	5.6.2.9 MF / DF.ESIGN / EF.C.HP.SIG.R2048	109
109	5.6.2.10 MF / DF.ESIGN / EF.C.HP.SIG.E256	111
110	5.6.2.11 MF / DF.ESIGN / PrK.HP.SIG.R2048	113
111	5.6.2.12 MF / DF.ESIGN / PrK.HP.SIG.E256	114
112	5.6.3 Sicherheitsumgebungen	115
113	5.7 Die kryptographischen Informationsanwendungen	116
114	5.7.1 MF / DF.CIA.QES (Cryptographic Information Applications)	116
115	5.7.1.1 MF / DF.CIA.QES / EF.CIA.CIAInfo	117
116	5.7.1.2 MF / DF.CIA.QES / EF.OD	120

117	5.7.1.3 MF / DF.CIA.QES / EF.AOD (Authentication Object Directory).....	122
118	5.7.1.4 MF / DF.CIA.QES / EF.PrKD (Private Key Directory)	125
119	5.7.1.5 MF / DF.CIA.QES / EF.CD (Certificate Directory).....	128
120	5.7.2 MF / DF.CIA.ESIGN (Cryptographic Information Applications)	130
121	5.7.2.1 MF / DF.CIA.ESIGN / EF.CIA.CIAInfo	131
122	5.7.2.2 MF / DF.CIA.ESIGN / EF.OD.....	135
123	5.7.2.3 MF / DF.CIA.ESIGN / EF.AOD (Authentication Object Directory)	137
124	5.7.2.4 MF / DF.CIA.ESIGN / EF.PrKD (Private Key Directory)	140
125	5.7.2.5 MF / DF.CIA.ESIGN / EF.CD (Certificate Directory)	145
126	5.8 Die Organisationsspezifische Authentisierungsanwendung	148
127	5.8.1 Dateistruktur und Dateiinhalt.....	148
128	5.8.2 DF.AUTO (Organization-specific Authentication Application).....	149
129	5.8.2.1 MF / DF.AUTO / PrK.HP.AUTO.R3072	151
130	5.8.2.2 MF / DF.AUTO / PIN.AUTO	153
131	5.8.2.3 MF / DF.AUTO / PIN.SO.....	156
132	5.8.2.4 MF / DF.AUTO / EF.C.HP.AUTO1.R3072 und MF / DF.AUTO /	
133	EF.C.HP.AUTO2.R3072	159
134	5.8.2.5 Sicherheitsumgebungen.....	164
135	5.8.2.6 Vorgaben für die Nutzung von DF.AUTO	164
136	5.9 Laden einer neuen Anwendung oder Anlegen eines EFs nach Ausgabe des	
137	HBA	165
138	6 Anhang A – Verzeichnisse	166
139	6.1 Abkürzungen	166
140	6.2 Glossar	172
141	6.3 Abbildungsverzeichnis	172
142	6.4 Tabellenverzeichnis	172
143	6.5 Referenzierte Dokumente	180
144	6.5.1 Dokumente der gematik.....	180
145	6.5.2 Weitere Dokumente.....	181
146	1 Einordnung des Dokumentes	9
147	1.1 Zielsetzung	9
148	1.2 Zielgruppe	9
149	1.3 Geltungsbereich	10
150	1.4 Abgrenzung des Dokuments	10
151	1.5 Methodik	10
152	1.5.1 Nomenklatur	10
153	1.5.2 Verwendung von Schlüsselworten	13
154	1.5.3 Komponentenspezifische Anforderungen	13
155	2 Optionen	14
156	2.1 Option Erstellung von Testkarten	14
157	3 Lebenszyklus von Karte und Applikation.....	15

4	Anwendungsübergreifende Festlegungen	16
4.1	Mindestanzahl logischer Kanäle	16
4.2	Unterstützung RSA CV-Zertifikate	16
4.3	Unterstützung Onboard-RSA-Schlüsselgenerierung	16
4.4	Unterstützung optionaler Funktionspakete	16
4.4.1	USB-Schnittstelle (optional)	16
4.4.2	Kontaktlose Schnittstelle (optional)	17
4.4.3	Kryptobox (optional)	18
4.4.4	Symmetrischer Kryptographiealgorithmus DES (optional)	18
4.5	Attributstabellen	19
4.5.1	Attribute eines Ordners	19
4.5.2	Attribute einer Datei (EF)	20
4.6	Zugriffsregeln für besondere Kommandos	20
4.7	Attributswerte und Personalisierung	21
4.8	Kartenadministration	22
5	Spezifikation grundlegender Applikationen	23
5.1	Attribute des Objektsystems	23
5.1.1	ATR-Kodierung	24
5.2	Allgemeine Struktur	25
5.3	Root, die Wurzelapplikation MF	25
5.3.1	MF / EF.ATR	27
5.3.2	MF / EF.CardAccess (Option kontaktlose Schnittstelle)	29
5.3.3	MF / EF.DIR	30
5.3.4	MF / EF.GDO	33
5.3.5	MF / EF.Version2	35
5.3.6	MF / EF.C.CA HPC.CS.E256	37
5.3.7	MF / EF.C.HPC.AUTR CVC.E256	39
5.3.8	MF / EF.C.HPC.AUTD SUK CVC.E256	41
5.3.9	MF / PIN.CH	44
5.3.10	MF / PrK.HPC.AUTR CVC.E256	46
5.3.11	MF / PrK.HPC.AUTD SUK CVC.E256	48
5.3.12	Sicherheitsanker zum Import von CV-Zertifikaten	51
5.3.12.1	MF / PuK.RCA.CS.E256	51
5.3.13	Asymmetrische Kartenadministration	54
5.3.13.1	MF / PuK.RCA.ADMINCMS.CS.E256	54
5.3.14	Symmetrische Kartenadministration	57
5.3.14.1	MF / SK.CMS.AES128	58
5.3.14.2	MF / SK.CMS.AES256	60
5.3.14.3	MF / SK.CUP.AES128	62
5.3.14.4	MF / SK.CUP.AES256	64
5.3.15	MF / SK.CAN (Option kontaktlose Schnittstelle)	66
5.3.16	Sicherheitsumgebungen auf MF-Ebene	68
5.4	Die Heilberufsanwendung DF.HPA	68
5.4.1	Dateistruktur und Dateinhalt	68
5.4.2	MF / DF.HPA (Health Professional Application)	68
5.4.2.1	MF / DF.HPA / EF.HPD (Health Professional Data)	70

204	5.4.2.2 Sicherheitsumgebungen	71
205	5.5 Die Anwendung für die qualifizierte elektronische Signatur (DF.QES)	72
206	5.5.1 Dateistruktur und Dateiinhalt.....	72
207	5.5.2 MF / DF.QES (Qualified Electronic Signature Application).....	72
208	5.5.2.1 MF / DF.QES / PrK.HP.QES.R2048	74
209	5.5.2.2 MF / DF.QES / PIN.QES.....	76
210	5.5.2.3 MF / DF.QES / EF.SSEC.....	79
211	5.5.2.4 MF / DF.QES / EF.C.HP.QES.R2048.....	82
212	5.5.2.5 MF / DF.QES / PrK.HP.QES.E256	84
213	5.5.2.6 MF / DF.QES / EF.C.HP.QES.E256.....	87
214	5.6 Die ESIGN-Anwendung (DF.ESIGN)	89
215	5.6.1 Dateistruktur und Dateiinhalt.....	89
216	5.6.2 MF / DF.ESIGN (Krypto-Anwendung ESIGN)	90
217	5.6.2.1 MF / DF.ESIGN / PrK.HP.AUT.R2048	91
218	5.6.2.2 MF / DF.ESIGN / PrK.HP.ENC.R2048	93
219	5.6.2.3 MF / DF.ESIGN / EF.C.HP.AUT.R2048.....	96
220	5.6.2.4 MF / DF.ESIGN / EF.C.HP.ENC.R2048.....	98
221	5.6.2.5 MF / DF.ESIGN / PrK.HP.AUT.E256	100
222	5.6.2.6 MF / DF.ESIGN / PrK.HP.ENC.E256	102
223	5.6.2.7 MF / DF.ESIGN / EF.C.HP.AUT.E256.....	105
224	5.6.2.8 MF / DF.ESIGN / EF.C.HP.ENC.E256	107
225	5.6.2.9 MF / DF.ESIGN / EF.C.HP.SIG.R2048	109
226	5.6.2.10 MF / DF.ESIGN / EF.C.HP.SIG.E256	111
227	5.6.2.11 MF / DF.ESIGN / PrK.HP.SIG.R2048.....	113
228	5.6.2.12 MF / DF.ESIGN / PrK.HP.SIG.E256.....	114
229	5.6.3 Sicherheitsumgebungen.....	115
230	5.7 Die kryptographischen Informationsanwendungen	116
231	5.7.1 MF / DF.CIA.QES (Cryptographic Information Applications)	116
232	5.7.1.1 MF / DF.CIA.QES / EF.CIA.CIAInfo.....	117
233	5.7.1.2 MF / DF.CIA.QES / EF.OD	120
234	5.7.1.3 MF / DF.CIA.QES / EF.AOD (Authentication Object Directory).....	122
235	5.7.1.4 MF / DF.CIA.QES / EF.PrKD (Private Key Directory)	125
236	5.7.1.5 MF / DF.CIA.QES / EF.CD (Certificate Directory).....	128
237	5.7.2 MF / DF.CIA.ESIGN (Cryptographic Information Applications)	130
238	5.7.2.1 MF / DF.CIA.ESIGN / EF.CIA.CIAInfo	131
239	5.7.2.2 MF / DF.CIA.ESIGN / EF.OD.....	135
240	5.7.2.3 MF / DF.CIA.ESIGN / EF.AOD (Authentication Object Directory)	137
241	5.7.2.4 MF / DF.CIA.ESIGN / EF.PrKD (Private Key Directory)	140
242	5.7.2.5 MF / DF.CIA.ESIGN / EF.CD (Certificate Directory)	145
243	5.8 Die Organisationsspezifische Authentisierungsanwendung	148
244	5.8.1 Dateistruktur und Dateiinhalt.....	148
245	5.8.2 DF.AUTO (Organization-specific Authentication Application).....	149
246	5.8.2.1 MF / DF.AUTO / PrK.HP.AUTO.R3072	151
247	5.8.2.2 MF / DF.AUTO / PIN.AUTO.....	153
248	5.8.2.3 MF / DF.AUTO / PIN.SO.....	156
249	5.8.2.4 MF / DF.AUTO / EF.C.HP.AUTO1.R3072	159
250	5.8.2.5 MF / DF.AUTO / EF.C.HP.AUTO2.R3072	162
251	5.8.2.6 Sicherheitsumgebungen.....	164
252	5.8.2.7 Vorgaben für die Nutzung von DF.AUTO	164
253	5.9 Laden einer neuen Anwendung oder Anlegen eines EFs nach Ausgabe des	
254	HBA	165

255	6 Anhang A – Verzeichnisse	166
256	6.1 Abkürzungen	166
257	6.2 Glossar	172
258	6.3 Abbildungsverzeichnis	172
259	6.4 Tabellenverzeichnis	172
260	6.5 Referenzierte Dokumente	180
261	6.5.1 Dokumente der gematik	180
262	6.5.2 Weitere Dokumente	181
263		

1 Einordnung des Dokumentes

1.1 Zielsetzung

Dieses Dokument spezifiziert die Objektstruktur des Heilberufsausweises (HBA) und beschreibt die Kartenschnittstelle zu dem HBA für Angehörige approbierter Heilberufe. Die Spezifikation ist so aufgebaut, dass sie an die Anforderungen anderer Heilberufe angepasst werden kann.

Die Spezifikation berücksichtigt:

- Die EU-Verordnung Nr. 910/2014 (eIDAS)
- die DIN-Spezifikation für Chipkarten mit digitaler Signatur
- die ESIGN-Spezifikation für elektronische Signaturen
- die zugehörigen ISO-Standards (speziell ISO/IEC 7816, Teile 1-4, 6, 8, 9 und 15)
- andere Quellen (z.B. Anforderungen der Trustcenter)

Die Spezifikation behandelt Anwendungen des elektronischen Heilberufsausweises (HBA) unter den folgenden, rein kartenorientierten Gesichtspunkten:

- Ordnerstruktur,
- Dateien,
- Sicherheitsmechanismen wie Zugriffsregeln.

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

1.2 Zielgruppe

Das Dokument richtet sich an

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

1.3 Geltungsbereich

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

Schutzrechts-/Patentrechtshinweis

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

1.4 Abgrenzung des Dokuments

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

Die „Äußere Gestaltung“ des HBA wird vom jeweils für die Ausgabe der HBAs verantwortlichen Sektor in eigener Verantwortung spezifiziert; dies ist nicht Aufgabe der gematik.

1.5 Methodik

1.5.1 Nomenklatur

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

In [gemSpec_COS] wurde ein objektorientierter Ansatz für die Beschreibung der Funktionalität des Betriebssystems gewählt. Deshalb wurde dort der Begriff "Passwortobjekt" verwendet, wenn Instanzen für eine Benutzerverifikation besprochen

wurden. Da in diesem Dokument lediglich numerische Ziffernfolgen als Verifikationsdaten eines Benutzers verwendet werden, wird hier statt Passwortobjekt vielfach der Begriff PIN gewählt, wenn keine Gefahr besteht, dass es zu Verwechslungen kommt zwischen den Verifikationsdaten und der Instanz des Objektes, in denen sie enthalten sind (zur Erinnerung: Ein Passwortobjekt enthält neben den Verifikationsdaten auch einen Identifier, eine Zugriffsregel, eine PUK, ...).

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

Für die Authentisierung der Zugriffe durch ein CMS auf die dafür vorgesehenen Objekte können entweder symmetrische Verfahren mit AES-Schlüsseln oder alternativ asymmetrische Verfahren mit CV-Zertifikaten verwendet werden. Für beide Verfahren sind die Schlüsselobjekte in dieser Spezifikation spezifiziert.

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

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

Beispiele:

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

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

AUT_CMS	{SmMac(SK.CMS.AES128) OR SmMac(SK.CMS.AES256) OR SmMac(flagCMS.08)} AND SmCmdEnc AND SmRspEnc
AUT_CUP	{SmMac(SK.CUP.AES128) OR SmMac(SK.CUP.AES256) OR SmMac(flagCMS.10)} AND SmCmdEnc AND SmRspEnc
AUT_PACE	SmMac(SK.CAN) AND SmCmdEnc AND SmRspEnc

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

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

1.5.2 Verwendung von Schlüsselworten

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

Sie werden im Dokument wie folgt dargestellt:

<AFO-ID> - <Titel der Afo>

Text / Beschreibung

[<=]

Dabei umfasst die Anforderung sämtliche innerhalb der Textmarken angeführten Inhalte.

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

1.5.3 Komponentenspezifische Anforderungen

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

Tabelle 1: Tab_HBA_ObjSys_001 Liste der Komponenten, an welche dieses Dokument Anforderungen stellt

Komponente	Beschreibung
K_Initialisierung	Instanz, welche eine Chipkarte im Rahmen der Initialisierung befüllt
K_Personalisierung	Instanz, welche eine Chipkarte im Rahmen der Produktion individualisiert
K_COS	Betriebssystem einer Smartcard

406

2 Optionen

407
408

Dieses Unterkapitel listet Funktionspakete auf, die für eine Zulassung eines HBA der Generation 2 nicht zwingend erforderlich sind.

409

2.1 Option_Erstellung_von_Testkarten

410
411
412
413
414
415

Card-G2-A_3319 - K_Personalisierung K_Initialisierung Vorgaben für die Option_Erstellung_von_Testkarten

Der HBA 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.

[<=]

416

3 Lebenszyklus von Karte und Applikation

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

420 Die Nutzungsphase einer Applikation oder eines Applikationsbestandteils beginnt, sobald
421 sich ein derartiges Objekt, wie in der Spezifikation der Anwendung definiert, verwenden
422 lässt. Die Nutzungsphase einer Applikation oder eines Applikationsbestandteils endet,
423 wenn das entsprechende Objekt gelöscht oder terminiert wird.
424

425 *Hinweis (1) Die in diesem Kapitel verwendeten Begriffe "Vorbereitungsphase" und*
426 *"Nutzungsphase" werden in [gemSpec_COS#4] definiert.*

ENTWURF

4 Anwendungsübergreifende Festlegungen

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

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

4.1 Mindestanzahl logischer Kanäle

Card-G2-A_2036 - K_Initialisierung Anzahl logischer Kanäle

Für die Anzahl logischer Kanäle, die von einem HBA zu unterstützen ist, gilt:

- a. Die maximale Anzahl logischer Kanäle MUSS gemäß [ISO7816-4#Tab.88] in den Historical Bytes in EF.ATR angezeigt werden.
- b. Der HBA MUSS mindestens vier logische Kanäle unterstützen. Das bedeutet, die in den Bits b3b2b1 gemäß [ISO7816-4#Tab.88] kodierte Zahl MUSS mindestens '011' = 3 oder größer sein.

[<=]

4.2 Unterstützung RSA CV-Zertifikate

A_15175 - K_HBA: Vorhandensein asymmetrischer Kryptographiealgorithmus RSA für CV-Zertifikate

Für einen HBA KANN für das Objektsystem ein COS verwendet werden

1. das die Option_RSA_CVC implementiert hat.
2. das die Option_RSA_CVC nicht implementiert hat.[<=]

4.3 Unterstützung Onboard-RSA-Schlüsselgenerierung

Card-G2-A_3848 - K_Personalisierung und K_Initialisierung: Unterstützung Onboard-RSA-Schlüsselgenerierung

Das COS eines HBA MUSS die Option_RSA_KeyGeneration implementieren.[<=]

4.4 Unterstützung optionaler Funktionspakete

4.4.1 USB-Schnittstelle (optional)

Card-G2-A_3006 - K_HBA: USB-Schnittstelle

Falls ein HBA die Option_USB_Schnittstelle nutzen will, MUSS für das Objektsystem ein COS verwendet werden, das die Option_USB_Schnittstelle implementiert hat.

[<=]

Card-G2-A_2867 - K_HBA: Vorhandensein einer USB-Schnittstelle

Falls ein HBA die Option_USB_Schnittstelle nicht nutzen will, KANN für das Objektsystem ein COS verwendet werden,

a. das die Option_USB_Schnittstelle implementiert hat.

b. das die Option_USB_Schnittstelle nicht implementiert hat.

[<=]

4.4.2 Kontaktlose Schnittstelle (optional)

Card-G2-A_3007 - K_HBA: Kontaktlose Schnittstelle

Falls ein HBA die Option_kontaktlose_Schnittstelle nutzen will, MUSS für das Objektsystem ein COS verwendet werden, das die Option_kontaktlose_Schnittstelle implementiert hat.

[<=]

Card-G2-A_2866 - K_HBA: Vorhandensein einer kontaktlosen Schnittstelle

Falls ein HBA die Option_kontaktlose_Schnittstelle nicht nutzen will, KANN für das Objektsystem ein COS verwendet werden,

a. das die Option_kontaktlose_Schnittstelle implementiert hat.

b. das die Option_kontaktlose_Schnittstelle nicht implementiert hat.

[<=]

Card-G2-A_3009 - K_HBA: Zusatzanforderungen für kontaktlose Schnittstelle

Falls ein HBA die Option_kontaktlose_Schnittstelle nutzen will, dann MÜSSEN zusätzlich zu allen nicht gekennzeichneten Anforderungen auch alle Anforderungen erfüllt sein, die mit Option_kontaktlose_Schnittstelle gekennzeichnet sind.

[<=]

Card-G2-A_3010 - K_Initialisierung und K_Personalisierung: Kontaktlose Schnittstelle wird nicht genutzt

Will der Kartenherausgeber eines HBA mit einem COS, das die Option_kontaktlose_Schnittstelle gemäß [gemSpec_COS] implementiert hat, die Nutzung dieser Schnittstelle verhindern, dann MUSS das Attribut *interfaceDependentAccessRules* aller Objekte so gesetzt sein, dass im Rahmen einer kontaktlosen Kommunikation die Zugriffsregelauswertung *AccessRuleEvaluation* (siehe [gemSpec_COS#10.4] stets den Wert „False“ liefert.

[<=]

Card-G2-A_3011 - K_Initialisierung: Kontaktlose Schnittstelle im COS nicht vorhanden

Falls das COS für einen HBA die Option_kontaktlose_Schnittstelle nicht implementiert hat, MUSS der Teil des Attributes *interfaceDependentAccessRules*, welcher sich auf die kontaktlose Kommunikation bezieht, für alle Objekte irrelevant für die Zulassung sein.

[<=]

Card-G2-A_3012 - K_Personalisierung: Absicherung der kontaktlosen Schnittstelle

Falls ein HBA die Option_kontaktlose_Schnittstelle nutzen will, MUSS die Kommunikation zwischen Karte und Kartenleser mit einer gegenseitigen Authentifizierung und Aufbau eines sicheren Kommunikationskanals abgesichert werden. Hierfür MUSS das PACE-Protokoll genutzt werden.

[<=]

Card-G2-A_2038 - K_Personalisierung: Druck der CAN auf den HBA bei Verwendung der optionalen kontaktlosen Schnittstelle

Falls ein HBA die Option_kontaktlose_Schnittstelle nutzen will, MUSS das Attribut *can* des Objektes SK.CAN mit der Nummer übereinstimmen, die auf dem HBA aufgedruckt ist.

[<=]

Card-G2-A_3277 - K_Personalisierung und K_Initialisierung: Konformität kontaktlose Schnittstelle

Ein HBA mit kontaktloser Schnittstelle MUSS in seiner endgültigen Konfiguration (einschließlich Kartenkörper und Antenne) bezüglich der elektrischen Eigenschaften dieser kontaktlosen Schnittstelle konform zu [ISO-IEC 14443] und [ISO/IEC FCD 10373-6] sein.

[<=]

4.4.3 Kryptobox (optional)

Card-G2-A_3014 - K_HBA: Vorhandensein Kryptobox

Für einen HBA KANN für das Objektsystem ein COS verwendet werden,

- a. das die Option_Kryptobox implementiert hat
- b. das die Option_Kryptobox nicht implementiert hat.

[<=]

4.4.4 Symmetrischer Kryptographiealgorithmus DES (optional)

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

Card-G2-A_3674 - K_HBA: Vorhandensein symmetrischer Kryptographiealgorithmus DES

Für einen HBA KANN für das Objektsystem ein COS verwendet werden,

1. das die Option_DES implementiert hat.
2. das die Option_DES nicht implementiert hat.

[<=]

4.5 Attributstabellen

Card-G2-A_2032 - K_Initialisierung: Änderung von Zugriffsregeln

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

[<=]

Card-G2-A_2329 - K_Initialisierung: Verhalten der Objekte, kein konkretes SE genannt

Falls für die SE abhängigen Attribute eines Objektes kein konkretes SE genannt ist, dann MUSS sich dieses Objekt in SE#1 wie angegeben verwenden lassen.

[<=]

Card-G2-A_3182 - K_Initialisierung: Verwendbarkeit der Objekte in anderen SEs, kein konkretes SE genannt

Falls für die SE abhängigen Attribute eines Objektes kein konkretes SE genannt ist, dann KANN dieses Objekt in SE verwendbar sein, die verschieden sind von SE#1.

[<=]

Card-G2-A_3183 - K_Initialisierung: Eigenschaften der Objekte in anderen SEs, kein konkretes SE genannt

Falls für die SE abhängigen Attribute eines Objektes kein konkretes SE genannt ist und dieses Objekt in einem von SE#1 verschiedenen SE verwendbar ist, dann MUSS es dort dieselben Eigenschaften wie in SE#1 besitzen.

[<=]

Card-G2-A_3184 - K_Initialisierung: Verhalten der Objekte, konkretes SE genannt

Falls für die SE abhängigen Attribute eines Objektes ein konkretes SE genannt ist, dann MUSS sich dieses Objekt dort wie angegeben verwenden lassen.

[<=]

Card-G2-A_3185 - K_Initialisierung: Verwendbarkeit der Objekte in anderen SEs, konkretes SE genannt

Falls für die SE abhängigen Attribute eines Objektes ein konkretes SE genannt ist, dann KANN dieses Objekt in SE verwendbar sein, die nicht konkret genannt sind.

[<=]

Card-G2-A_3186 - K_Initialisierung: Eigenschaften der Objekte in anderen SEs, konkretes SE genannt

Falls für die SE abhängigen Attribute eines Objektes ein konkretes SE genannt ist und dieses Objekt ist in einem nicht konkret angegebenen SE verwendbar, dann MUSS es dort dieselben Eigenschaften wie in einem konkret angegebenen besitzen.

[<=]

4.5.1 Attribute eines Ordners

Card-G2-A_2033-01 - K_Initialisierung: Ordnerattribute

Enthält eine Tabelle mit Ordnerattributen einen oder mehrere applicationIdentifier (AID), dann MUSS sich dieser Ordner mittels aller angegebenen AID selektieren lassen

[<=]

Card-G2-A_3624 - K_Initialisierung: Herstellerspezifischer ApplicationIdentifier

Enthält eine Tabelle mit Ordnerattributen keinen *applicationIdentifier* (AID), so KANN diesem Ordner herstellerspezifisch ein beliebiger AID zugeordnet werden.

[<=]

Card-G2-A_3625 - K_Initialisierung: Fehlender FileIdentifier

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

[<=]

Card-G2-A_3626 - K_Initialisierung: Herstellerspezifischer FileIdentifier

Enthält eine Tabelle mit Ordnerattributen keinen *fileIdentifier* (FID), so KANN diesem Ordner ein beliebiger *fileIdentifier* außerhalb des Intervalls gemäß [gemSpec_COS#8.1.1] zugeordnet werden.

[<=]

4.5.2 Attribute einer Datei (EF)

Card-G2-A_2034 - K_Initialisierung: Dateiattribute

Enthält eine Tabelle mit Attributen einer Datei keinen *shortFileIdentifier*, so DARF sich dieses EF NICHT mittels *shortFileIdentifier* aus dem Intervall gemäß [gemSpec_COS#8.1.2] selektieren lassen.

[<=]

Card-G2-A_2673 - K_Personalisierung und K_Initialisierung: Wert von „positionLogicalEndOfFile“

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

[<=]

4.6 Zugriffsregeln für besondere Kommandos

Card-G2-A_2035 - K_Initialisierung: Zugriffsregeln für besondere Kommandos

Für Kommandos, für die eine Zugriffsregelauswertung gemäß [gemSpec_COS] optional ist, werden nicht in den Attributstabellen, sondern zentral in dieser Anforderung die Zugriffsbedingungen festgelegt:

- a. Für die kontaktbehaftete Schnittstelle MUSS die Zugriffsbedingung für die Kommandos GET CHALLENGE, LIST PUBLIC KEY, MANAGE SECURITY ENVIRONMENT und SELECT stets ALWAYS sein.
- b. Falls der HBA die Option_kontaktlose_Schnittstelle unterstützt, dann MUSS die Zugriffsbedingung für die Kommandos GET CHALLENGE, LIST PUBLIC KEY, MANAGE SECURITY ENVIRONMENT und SELECT stets ALWAYS sein.
- c. Falls ein Kartenherausgeber die Nutzung einer im COS vorhandenen kontaktlosen Schnittstelle unterbinden will, dann MUSS die Zugriffsbedingung für die Kommandos GET CHALLENGE, LIST PUBLIC KEY, MANAGE SECURITY

627 ENVIRONMENT und SELECT für die kontaktlose Schnittstelle
628 herstellerspezifisch stets entweder ALWAYS oder NEVER sein.

629
630 [\leq]

631 4.7 Attributswerte und Personalisierung

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

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

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

657 Die folgende Anforderung ermöglicht herstellerspezifische Personalisierungsprozesse:

658

659 **Card-G2-A_3325 - K_Initialisierung und K_Personalisierung: Abweichung von** 660 **Festlegungen zum Zwecke der Personalisierung**

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

666 [\leq]

667 Für die Initialisierung und Personalisierung asymmetrischer Schlüssel gelten folgende
668 Anforderungen:

669 **Card-G2-A_3525 - K_Initialisierung: Schlüsselgenerierung auf der Karte**

670 Der HBA MUSS die Generierung von asymmetrischen Schlüsselpaaren auf der Karte
671 ermöglichen.

672 [\leq]

Card-G2-A_3526 - K_Initialisierung: Weitere Verfahren zur Personalisierung von Schlüsseln

Der HBA KANN andere Verfahren als das in Card-G2-A_3525 genannte zur Personalisierung asymmetrischer Schlüsselpaare unterstützen.

[<=]

Card-G2-A_3523 - K_Personalisierung: Schlüsselgenerierung auf der Karte

Wenn ein privater Schlüssel für den HBA zu personalisieren ist, dann MUSS das Schlüsselpaar von der Smartcard selbst erzeugt werden. Es MUSS sichergestellt sein, dass der private Teil des Schlüssels die Smartcard nie verlässt.

[<=]

4.8 Kartenadministration

In den Kapiteln 5.3.16 und 5.3.17 sind die Objekte für die zwei verschiedenen Verfahren zur Absicherung der Kommunikation zwischen einem Kartenadministrationssystem (z.B. einem CUPs) und einer Karte beschrieben, die bei der Ausgabe der Karte angelegt werden müssen.

Card-G2-A_3005 - Absicherung der Kartenadministration

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

[<=]

Card-G2-A_3590 - Symmetrische Kartenadministration

Bei der Personalisierung KÖNNEN die Schlüssel (SK.CMS und SK.CUP) für die symmetrische Authentifizierung des Kartenadministrationssystems in die Karte eingebracht werden.

[<=]

Card-G2-A_3591 - Schlüsselspeicherung

Der Kartenherausgeber MUSS sicherstellen, dass die Schlüssel zur Absicherung der Kartenadministration während der gesamten Nutzungsdauer des HBA sicher verwahrt werden und bei Bedarf an ein Kartenadministrationssystem (z.B. ein CUPs) übergeben werden können.

[<=]

5 Spezifikation grundlegender Applikationen

Zu den grundlegenden Applikationen des elektronischen Heilberufsausweises (HBA) zählen:

- das Wurzelverzeichnis des HBA, auch root oder Master File (MF) genannt,
- die Gesundheitsanwendung DF.HPA (Health Professional Application),
- die Krypto-Anwendung DF.QES
- die Beschreibung kryptographischer Objekte DF.CIA.QES
- die Krypto-Anwendung DF.ESIGN
- die Beschreibung kryptographischer Objekte DF.CIA.ESIGN
- die organisationsspezifische Anwendung DF.AUTO.

5.1 Attribute des Objektsystems

Das Objektsystem [gemSpec_COS] enthält folgende Attribute:

Card-G2-A_2039 - K_Initialisierung: Wert des Attributes root

Der Wert des Attributes *root* MUSS die Anwendung gemäß Tab_HBA_ObjSys_004 sein.
[<=]

Card-G2-A_2040-01 - K_Personalisierung und K_Initialisierung: Wert des Attributes answerToReset

Die Werte der Attribute *coldAnswerToReset* und *warmAnswerToReset* MÜSSEN den Vorgaben der Anforderungen Card-G2-A_2043, Card-G2-A_2044-01, Card-G2-A_3627, Card-G2-A_2045 und Card-G2-A_3015 entsprechen.
[<=]

Card-G2-A_2041 - K_Personalisierung: Wert des Attributes iccsn8

Der Wert des Attributes *iccsn8* MUSS identisch zu den letzten acht Oktetts im *body* von EF.GDO sein.
[<=]

Card-G2-A_2042-01 - K_Initialisierung: Inhalt persistentPublicKeyList

Das Attribut *persistentPublicKeyList* MUSS den Schlüssel PuK.RCA.CS.E256 enthalten.[<=]

Card-G2-A_3181 - K_Initialisierung: Größe persistentPublicKeyList

Für das Attribut *persistentPublicKeyList* MUSS so viel Speicherplatz bereitgestellt werden, dass mindestens fünf weitere öffentliche Signaturprüfchlüssel einer Root-CA mittels Linkzertifikaten persistent importierbar sind.
[<=]

Card-G2-A_3266-01 - K_Initialisierung: Wert von pointInTime

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

Card-G2-A_3395 - K_Personalisierung: personalisierter Wert von pointInTime

Das Attribut *pointInTime* MUSS im Rahmen der Personalisierung auf den Wert von CED eines Endnutzerzertifikates gesetzt werden. Falls es mehrere Endnutzerzertifikate gibt, so ist das CED mit dem größten Wert zu verwenden.

[<=]

5.1.1 ATR-Kodierung

Card-G2-A_2043 - K_Personalisierung und K_Initialisierung: ATR-Kodierung

Die ATR-Kodierung MUSS die in Tab_HBA_ObjSys_003 dargestellten Werte besitzen.

Tabelle 2: Tab_HBA_ObjSys_003 ATR-Kodierung (Sequenz von oben nach unten)

Zeichen	Wert	Bedeutung
TS	'3B'	Initial Character (direct convention)
T0	'9x'	Format Character (TA1/TD1 indication, x = no. of HB)
TA1	'xx'	Interface Character (FI/DI, erlaubte Werte: siehe [gemSpec_COS#N024.100])
TD1	'81'	Interface Character, (T=1, TD2 indication)
TD2	'B1'	Interface Character, (T=1, TA3/TB3/TD3 indication)
TA3	'FE'	Interface Character (IFSC coding)
TB3	'45'	Interface Character, (BWI/CWI coding)
TD3	'1F'	Interface Character, (T=15, TA4 indication)
TA4	'xx'	Interface Character (XI/UI coding)
Ti	HB	Historical Bytes (HB, imax. = 15)
TCK	XOR	Check Character (exclusive OR)

[<=]

Card-G2-A_2044-01 - K_Personalisierung und K_Initialisierung: TC1 Byte im ATR

Der ATR SOLL ein TC1 Byte mit dem Wert 'FF' enthalten.

[<=]

Card-G2-A_3627 - K_Personalisierung und K_Initialisierung: T0 Byte im ATR

Wenn der ATR ein TC1 Byte mit dem Wert 'FF' enthält, MUSS T0 auf den Wert 'Dx' gesetzt werden.

[<=]

Card-G2-A_3015 - K_Personalisierung und K_Initialisierung: Historical Bytes im ATR

Das Attribut *answerToReset* SOLL KEINE Historical Bytes enthalten.

[<=]

Card-G2-A_2045 - K_Personalisierung und K_Initialisierung: Vorgaben für Historical Bytes

Falls answerToReset Historical Bytes enthält, dann MÜSSEN

a. diese gemäß [ISO7816-4] kodiert sein.

b. die dort getroffenen Angaben konsistent sein zu Angaben im EF.ATR.

[<=]

5.2 Allgemeine Struktur

Abb_HBA_ObjSys_001 zeigt die allgemeine Struktur der Objekte eines HBA.

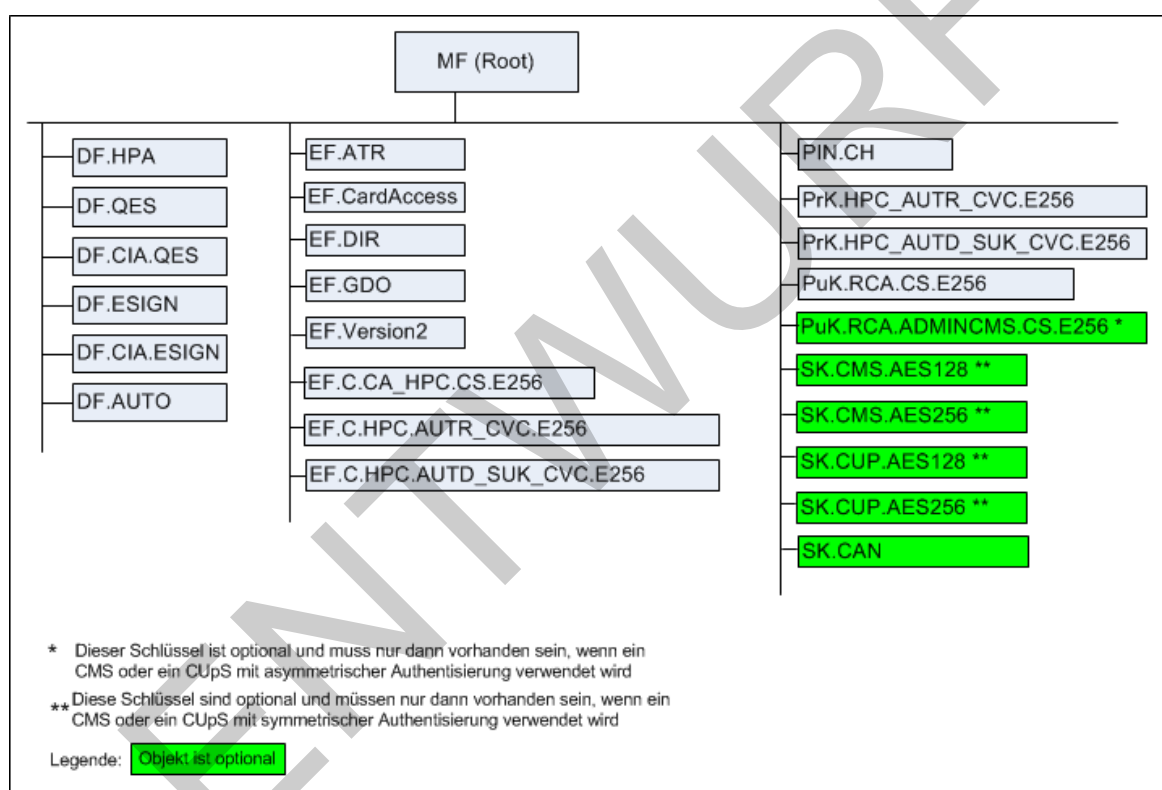


Abbildung 1: Abb_HBA_ObjSys_001 Allgemeine Dateistruktur eines HBA

5.3 Root, die Wurzelapplikation MF

MF ist ein „Application Dedicated File“ (siehe [gemSpec_COS#8.3.1.3]).

Card-G2-A_2047-01 - K_Initialisierung: Initialisierte Attribute von MF

MF MUSS die in Tab_HBA_ObjSys_004 dargestellten Werte besitzen.

Tabelle 3: Tab_HBA_ObjSys_004 Initialisierte Attribute von MF

Attribute	Wert	Bemerkung
-----------	------	-----------

Objekttyp	Ordner	
<i>applicationIdentifier</i>	'D27600014601'	
<i>fileIdentifier</i>	'3F 00'	falls vorhanden
<i>lifeCycleStatus</i>	„Operational state (activated)“	
<i>shareable</i>	True	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
FINGERPRINT	Wildcard	
GET RANDOM	ALWAYS	
LOAD APPLICATION	AUT_CMS	siehe Hinweis 4:
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	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
GET RANDOM	AUT_PACE	
LOAD APPLICATION	AUT_CMS	siehe Hinweis 4:
andere	NEVER	

Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

[<=]

Hinweis (2) Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten, sind:

Activate, Deactivate, Delete, Fingerprint, Get Random, List Public Key, Load Application, Select, Terminate DF.

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

Hinweis (4) Nur dann ausführbar, wenn ein CMS genutzt wird (optional), siehe Kapitel 5.9

5.3.1 MF / EF.ATR

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

Card-G2-A_2048-01 - K_Initialisierung: Initialisierte Attribute von MF / EF.ATR
EF.ATR MUSS die in Tab_HBA_ObjSys_005 dargestellten Werte besitzen.

Tabelle 4: Tab_HBA_ObjSys_005 Initialisierte Attribute von MF / EF.ATR

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	'2F 01'	siehe Hinweis (6÷)
shortFileIdentifier	'1D' = 29	
numberOfOctet	herstellerspezifisch Wildcard	siehe Card-G2-A 3278
positionLogicalEndOfFile	Wildcard Zahl der tatsächlich belegten Oktette	siehe Card-G2-A 2673
flagTransactionMode	True	

flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
body	Inhalt gemäß [gemSpec_Karten_Fach_TIP_G2.1]	siehe unten
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
Read Binary Write Binary	ALWAYS	
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	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
Read Binary Write Binary	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

810

811 [<=]

812 Hinweis (5) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF
813 arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Set
814 Logical Eof, Update Binary, Terminate, Write Binary.

815 Hinweis (6) Der Wert des Attributs *fileIdentifier* ist in [ISO7816-4] festgelegt.

816 **Card-G2-A_3278 - K_Initialisierung: Initialisiertes Attribut numberOfOctet von** 817 **MF / EF.ATR**

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

- 820 • genau 23 Oktette für die Artefakte PT_Pers und PI_Personalisierung frei bleiben,
821 falls PI_Kartenkörper initialisiert wird, oder
- 822 • genau 41 Oktette für die Artefakte PI_Kartenkörper, PT_Pers und
823 PI_Personalisierung frei bleiben.

824 [\leq]

825 **5.3.2 MF / EF.CardAccess (Option kontaktlose Schnittstelle)**

826 EF.CardAccess wird für das PACE-Protokoll bei Nutzung der kontaktlosen Schnittstelle
827 benötigt.

828 **Card-G2-A_3199-01Card-G2-A_3199 - K_Initialisierung: Initialisierte Attribute** 829 **von MF / EF.CardAccess**

830 Falls die kontaktlose Schnittstelle für den HBA genutzt wird, MUSS EF.CardAccess
831 vorhanden sein und die in Tab_HBA_ObjSys_083 dargestellten Attribute besitzen.

832 **Tabelle 5: Tab_HBA_ObjSys_083 Initialisierte Attribute von MF / EF.CardAccess**

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
<i>fileIdentifier</i>	'01 1C'	
<i>shortFileIdentifier</i>	'1C' = 28	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
<i>flagTransactionMode</i>	False	
<i>flagChecksum</i>	True	
<i>numberOfOctet</i>	Wildcard <u>passend zum Inhalt</u>	<u>passend zum Inhalt</u>
<i>positionLogicalEndOfFile</i>	passend zum Inhalt <u>Wildcard</u>	<u>siehe Card-G2-A_2673</u>
<i>shareable</i>	True	

body	passend zu den Attributen von SK.CAN gemäß [TR-03110-3]	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsart	Zugriffsbedingung	Bemerkung
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
READ BINARY	ALWAYS	

andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktbehaftet		
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Operational state (terminated)“ kontaktbehaftet		
alle	herstellerspezifisch	

Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
READ BINARY	ALWAYS	

andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Operational state (terminated)“ kontaktlos		
alle	herstellerspezifisch	

[<=]

[<=]

5.3.3 MF / EF.DIR

Die Datei enthält eine Liste mit Anwendungs-Templates gemäß [ISO7816-4]. Diese Liste wird dann angepasst, wenn sich die Applikationsstruktur durch Löschen oder Anlegen von

840 Anwendungen verändert.
841

842 **Card-G2-A_3628 - K_Initialisierung: Inhalt der Records von EF.DIR**

843 Für jede im Objektsystem vorhandene Anwendung MUSS die Datei einen eigenen Record
844 besitzen, der den ApplicationIdentifier (AID) dieser Anwendung im Format '61-L61-
845 {4F-L4F-AID}' enthält.

846 Zu jedem Record der Datei MUSS es auf der Karte eine Anwendung geben, deren AID
847 durch diesen Record beschrieben ist.

848 Record 1 des EF.DIR MUSS den AID des MF enthalten.

849 [\leq]

850 **Card-G2-A_2055-01 - K_Initialisierung: Initialisierte Attribute von MF / EF.DIR**

851 EF.DIR MUSS die in Tab_HBA_ObjSys_007 dargestellten Werte besitzen.

852

853 **Tabelle 6: Tab_HBA_ObjSys_007 Initialisierte Attribute von MF / EF.DIR**

Attribute	Wert	Bemerkung
Objekttyp	linear variables Elementary File	
<i>fileIdentifier</i>	'2F 00'	Siehe Hinweis 8:
<i>shortFileIdentifier</i>	'1E' = 30	Siehe Hinweis 8:
<i>numberOfOctet</i>	'00 BE' Oktett = 190 Oktett	
<i>maxNumRecords</i>	10 Records	
<i>maxRecordLength</i>	32 Oktett	
<i>flagRecordLCS</i>	False	
<i>flagTransactionMode</i>	True	
<i>flagChecksum</i>	True	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
<i>shareable</i>	True	
<i>recordList</i> Record 1 Record 2 und folgende	'61- 08- (4F 06 D27600014601)' '61-L61-{4F-L4F-AID}' für alle Applikationen im Objektsystem	AID.MF
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
Append Record	AUT_CMS	siehe Hinweis 8:.
Delete Record	AUT_CMS	siehe Hinweis 8:

Read Record Search Record	ALWAYS	
Update Record	AUT_CMS	siehe Hinweis 8:
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	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
Append Record	AUT_CMS	siehe Hinweis 9:
Delete Record	AUT_CMS	siehe Hinweis 9:
Read Record Search Record	AUT_PACE OR AUT_CMS	
Update Record	AUT_CMS	siehe Hinweis 9:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

854

855 [**<=**]

856 *Hinweis (7) Kommandos, die gemäß [gemSpec_COS] mit einem linear variablen EF*
857 *arbeiten, sind:*

858 *Activate, Activate Record, Append Record, Deactivate, Deactivate Record, Delete, Delete*
859 *Record, Erase Record, Read Record, Search Record, Select, Terminate, Update Record,*
860 *Write Record.*

861 *Hinweis (8) Die Werte von fileIdentifier und shortFileIdentifier sind in [ISO7816-4]*
862 *festgelegt.*

863 Hinweis (9) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar,
864 siehe Kapitel 5.9.

865 5.3.4 MF / EF.GDO

866 In EF.GDO wird das Datenobjekt ICCSN gespeichert, das die Kennnummer der Karte
867 enthält. Die Kennnummer basiert auf [Beschluss 190].

868 [Card-G2-A 2057-01](#) ~~Card-G2-A-2057~~ - K_Initialisierung: Initialisierte Attribute
869 von MF / EF.GDO

870 EF.GDO MUSS die in Tab_HBA_ObjSys_008 dargestellten Werte besitzen.

871 **Tabelle 7: Tab_HBA_ObjSys_008 Initialisierte Attribute von MF / EF.GDO**

Attribute	Wert	Bemerkung
Objektyp	transparentes Elementary File	
fileIdentifier	'2F 02'	
shortFileIdentifier	'02' = 2	
numberOfOctet	'00 0C' Oktett = 12 Oktett	
positionLogicalEndOfFile	'0' Wildcard	siehe Card-G2-A 2673
flagTransactionMode	False	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
body	Wildcard	wird personalisiert
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	ALWAYS	
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	

Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)

Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos

Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	AUT_PACE	

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

[<=]

Hinweis (10) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Set Logical Eof, Update Binary, Terminate, Write Binary.

Card-G2-A_2058-01 - K_Personalisierung: Personalisiertes Attribut von EF.GDO
Bei der Personalisierung von EF.GDO MÜSSEN die in Tab_HBA_ObjSys_151 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 8: Tab_HBA_ObjSys_151 Personalisierte Attribute von MF / EF.GDO

Attribute	Wert	Bemerkung
positionLogicalEndOfFile	'00 0C' Oktett = 12 Oktett	

<i>body</i>	Inhalt gemäß [gemSpec_Karten_Fach_TIP_G2.1]	
-------------	--	--

883

884 [\leq]

885 5.3.5 MF / EF.Version2

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

- 888 • Version des Produkttyps des aktiven Objektsystems (inkl. Kartenkörper
- 889 • Herstellerspezifische Produktidentifikation der Objektsystemimplementierung
- 890 • Versionen der Befüllvorschriften für verschiedene Dateien dieses
- 891 Objektsystems

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

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

895

896 Card-G2-A 2059-02~~Card-G2-A-2059-01~~ - K_Initialisierung: Attribute von MF /
897 EF.Version2

898 EF.Version2 MUSS die in Tab_HBA_ObjSys_009 dargestellten Werte besitzen.

899 **Tabelle 9: Tab_HBA_ObjSys_009 Initialisierte Attribute von MF / EF.Version2**

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
<i>fileIdentifier</i>	'2F 11'	
<i>shortFileIdentifier</i>	'11' = 17	
<i>numberOfOctet</i>	'00 3C' Oktett = 60 Oktett	
<i>positionLogicalEndOfFile</i>	passend zum Inhalt <u>Wildcard</u>	<u>siehe Card-G2-A 2673</u>
<i>flagTransactionMode</i>	True	
<i>flagChecksum</i>	True	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
<i>shareable</i>	True	

body	Inhalt gemäß [gemSpec_Karten_Fach_TIP_G2.1]	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
Read Binary	ALWAYS	
Update Binary Set Logical EOF	AUT_CMS	siehe Hinweis (12÷)
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
Read Binary	ALWAYS	
Update Binary Set Logical EOF	AUT_CMS	siehe Hinweis (12÷)
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

[<=]

Hinweis (11) 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.

905 Hinweis (12) Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe
906 Kapitel 5.9.

907

908 5.3.6 MF / EF.C.CA_HPC.CS.E256

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

912 [Card-G2-A 2061-01](#) ~~Card-G2-A-2061~~ - K_Initialisierung: Initialisierte Attribute
913 von MF / EF.C.CA_HPC.CS.E256

914 EF.C.CA_HPC.CS.E256 MUSS die in Tab_HBA_ObjSys_011 dargestellten Werte besitzen.

915 **Tabelle 10: Tab_HBA_ObjSys_011 Initialisierte Attribute von MF / EF.C.CA_HPC.CS.E256**

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	'2F 07'	
shortFileIdentifier	'07' = 7	
numberOfOctet	'00 DC' Oktett = 220 Oktett	
positionLogicalEndOfFile	'0' Wildcard	siehe Card-G2-A 2673
flagTransactionMode	True	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
body	kein Inhalt	wird personalisiert
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE UPDATE BINARY	AUT_CMS OR AUT_CUP	siehe Hinweis (14÷)

READ	BINARY	ALWAYS	
UPDATE BINARY	AUT_CMS OR AUT_CUP		siehe Hinweis 14:
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		
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)			
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos			
Zugriffsart	Zugriffsbedingung	Bemerkung	
DELETE <u>UPDATE BINARY</u>	AUT_CMS OR AUT_CUP	siehe Hinweis (14:)	
READ	BINARY	AUT_PAGE OR AUT_CMS OR AUT_CUP <u>OR</u> <u>AUT_PAGE</u>	
UPDATE BINARY	AUT_CMS OR AUT_CUP		siehe Hinweis 14:
andere	NEVER		
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos			
Zugriffsart	Zugriffsbedingung	Bemerkung	
alle	herstellerspezifisch		
Zugriffsregel für logischen LCS „Termination state“ kontaktlos			
Zugriffsart	Zugriffsbedingung	Bemerkung	
alle	herstellerspezifisch		

[<=]

Hinweis (14) Das Kommando ist nur vom Inhaber des CMS- /CUP-Schlüssels ausführbar, siehe Kapitel 5.9.

Card-G2-A_3282 - K_Personalisierung: Personalisierte Attribute von MF / EF.C.CA_HPC.CS.E256

Bei der Personalisierung von EF.C.CA_HPC.CS.E256 MÜSSEN die in Tab_HBA_ObjSys_090 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 11: Tab_HBA_ObjSys_090 Personalisierte Attribute von MF / EF.C.CA_HPC.CS.E256

Attribute	Wert	Bemerkung
<i>positionLogicalEndOfFile</i>	'00 DC' Oktett = 220 Oktett	
<i>body</i>	C.CA_HPC.CS.E256 gemäß [gemSpec_PKI#6.7.1]	siehe [gemSpec_COS]
<i>body</i> <i>Option_Erstellung_von_Testkarten</i>	C.CA_HPC.CS.E256 gemäß [gemSpec_PKI#6.7.1] aus Test-CVC-CA	Details siehe [gemSpec_TK#3.1.2]

[<=]

5.3.7 MF / EF.C.HPC.AUTR_CVC.E256

EF.C.HPC.AUTR_CVC.E256 enthält das CV-Zertifikat des HBA für die Kryptographie mit elliptischen Kurven für rollenbasierte C2C-Authentisierung zwischen HBA und eGK und für die Autorisierung der SMC-B. Dieses Zertifikat lässt sich mittels des öffentlichen Schlüssels aus EF.C.CA_HPC.CS.E256 (siehe Tab_HBA_ObjSys_011) prüfen. Das zugehörige private Schlüsselobjekt PrK.HPC.AUTR_CVC.E256 ist im Kapitel 5.3.13 definiert.

Card-G2-A 2064-01 ~~Card-G2-A-2064~~ - K_Initialisierung: Initialisierte Attribute von MF / EF.C.HPC.AUTR_CVC.E256

EF.C.HPC.AUTR_CVC.E256 MUSS die in Tab_HBA_ObjSys_014 dargestellten Werte besitzen.

Tabelle 12: Tab_HBA_ObjSys_014 Initialisierte Attribute von MF / EF.C.HPC.AUTR_CVC.E256

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
<i>fileIdentifier</i>	'2F 06'	
<i>shortFileIdentifier</i>	'06' = 6	
<i>numberOfOctet</i>	'00 DE' Oktett = 222 Oktett	
<i>positionLogicalEndOfFile</i>	'0' Wildcard	siehe Card-G2-A 2673
<i>flagTransactionMode</i>	True	
<i>flagChecksum</i>	False	

lifeCycleStatus	„Operational state (activated)“	
shareable	True	
body	kein Inhalt	wird personalisiert
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE <u>UPDATE BINARY</u>	AUT_CMS OR AUT_CUP	siehe Hinweis <u>(18÷)</u>
READ BINARY	ALWAYS	
UPDATE BINARY	AUT_CMS OR AUT_CUP	siehe Hinweis 18÷
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	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE <u>UPDATE BINARY</u>	AUT_CMS OR AUT_CUP	siehe Hinweis <u>(18÷)</u>
READ BINARY	<u>AUT_PACE</u> OR AUT_CMS OR AUT_CUP <u>OR AUT_PACE</u>	
UPDATE BINARY	AUT_CMS OR AUT_CUP	siehe Hinweis 18÷
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung

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

[<=]

Hinweis (17) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Set Logical Eof, Update Binary, Terminate, Write Binary.

Hinweis (18) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.9.

Card-G2-A_3386 - K_Personalisierung: Festlegung von CHR in MF / EF.C.HPC.AUTR_CVC.E256

Für die CHR in diesem Zertifikat MUSS CHR = '00 06' || ICCSN gelten, wobei die ICCSN denselben Wert besitzen MUSS, wie das Wertfeld *body* aus [Card-G2-A_2058].

[<=]

Card-G2-A_3284 - K_Personalisierung: Personalisierte Attribute von MF / EF.C.HPC.AUTR_CVC.E256

Bei der Personalisierung von EF.C.HPC.AUTR_CVC.E256 MÜSSEN die in Tab_HBA_ObjSys_093 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 13: Tab_HBA_ObjSys_093 Personalisierte Attribute von MF / EF.C.HPC.AUTR_CVC.E256

Attribute	Wert	Bemerkung
<i>positionLogicalEndOfFile</i>	'00 DE' Oktett = 222 Oktett	
<i>body</i>	C.HPC.AUTR_CVC.E256 gemäß [gemSpec_PKI]	

[<=]

5.3.8 MF / EF.C.HPC.AUTD_SUK_CVC.E256

EF.C.HPC.AUTD_SUK_CVC.E256 enthält das CV-Zertifikat des HBA für die Kryptographie mit elliptischen Kurven für funktionsbasierte C2C-Authentisierung zwischen HBA/gSMC-KT und HBA/gSMC-K mit dem HBA als Signaturkarte für Stapel- und Komfortsignaturen (SUK), um PIN-Daten und die zu signierenden Daten (DTBS) zu empfangen. Das zugehörige private Schlüsselobjekt PrK.HPC.AUTD_SUK_CVC.E256 ist im Kapitel 5.3.14 definiert.

Card-G2-A 2067-01 - K_Initialisierung: Initialisierte Attribute von MF / EF.C.HPC.AUTD_SUK_CVC.E256

EF.C.HPC.AUTD_SUK_CVC.E256 MUSS die in Tab_HBA_ObjSys_017 dargestellten Werte besitzen.

Tabelle 14: Tab_HBA_ObjSys_017 Initialisierte Attribute von MF / EF.C.HPC.AUTD_SUK_CVC.E256

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
<i>fileIdentifier</i>	'2F 09'	
<i>shortFileIdentifier</i>	'09' = 9	
<i>numberOfOctet</i>	'00 DE' Oktett = 222 Oktett	
<i>positionLogicalEndOfFile</i>	'0' Wildcard	siehe Card-G2-A 2673
<i>flagTransactionMode</i>	True	
<i>flagChecksum</i>	False	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
<i>shareable</i>	True	
<i>body</i>	kein Inhalt	wird personalisiert
Zugriffsregeln		
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE UPDATE BINARY	AUT_CMS OR AUT_CUP	siehe Hinweis (20÷)
READ BINARY	ALWAYS	
SELECT	ALWAYS	
UPDATE BINARY	AUT_CMS OR AUT_CUP	siehe Hinweis 20÷

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	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE <u>UPDATE BINARY</u>	AUT_CMS OR AUT_CUP	siehe Hinweis <u>(20÷)</u>
READ BINARY	<u>AUT_PACE</u> OR <u>AUT_CMS OR AUT_CUP</u> OR <u>AUT_CUPPACE</u>	
<u>UPDATE BINARY</u>	<u>AUT_CMS OR AUT_CUP</u>	siehe Hinweis 20÷
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

[<=]

Hinweis (19) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Set Logical Eof, Update Binary, Terminate, Write Binary.

Hinweis (20) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.9.

Card-G2-A_3387 - K_Personalisierung: Festlegung von CHR in MF / EF.C.HPC.AUTD_SUK_CVC.E256

Für die CHR in diesem Zertifikat MUSS CHR = '00 09' || ICCSN gelten, wobei die ICCSN denselben Wert besitzen MUSS, wie das Wertfeld *body* aus [Card-G2-A_2058].
[<=]

Card-G2-A_3285 - K_Personalisierung: Personalisierte Attribute von MF / EF.C.HPC.AUTD_SUK_CVC.E256

Bei der Personalisierung von EF.C.HPC.AUTD_SUK_CVC.E256 MÜSSEN die in Tab_HBA_ObjSys_095 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 15: Tab_HBA_ObjSys_095 Personalisierte Attribute von MF / EF.C.HPC.AUTD_SUK_CVC.E256

Attribute	Wert	Bemerkung
positionLogicalEndOfFile	'00 DE' Oktett = 222 Oktett	
body	C.HPC.AUTD_SUK_CVC.E256 gemäß [gemSpec_PKI] passend zu dem privaten Schlüssel in PrK.HPC.AUTD_SUK_CVC.E256	

[<=]

5.3.9 MF / PIN.CH

Das Passwortobjekt PIN.CH wird zur Freischaltung von Schlüsseln und Inhalten des HBA verwendet.

Card-G2-A_2069 - K_Initialisierung: Initialisierte Attribute von MF / PIN.CH

PIN.CH MUSS die in Tab_HBA_ObjSys_019 dargestellten Werte besitzen.

Tabelle 16: Tab_HBA_ObjSys_019 Initialisierte Attribute von MF / PIN.CH

Attribute	Wert	Bemerkung
Objekttyp	Passwortobjekt	
<i>pwdIdentifier</i>	'01' = 1	
<i>secret</i>	undefiniert	wird personalisiert
<i>minimumLength</i>	6	
<i>maximumLength</i>	8	
<i>startRetryCounter</i>	3	
<i>retryCounter</i>	3	
<i>transportStatus</i>	Transport-PIN	
<i>flagEnabled</i>	True	
<i>startSsec</i>	unendlich	

<i>PUK</i>	undefiniert	wird personalisiert
<i>pukUsage</i>	10	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
CHANGE RD, P1=0	ALWAYS	
GET PIN STATUS	ALWAYS	
RESET RC. P1 aus der Menge {0, 1}	ALWAYS	
VERIFY	ALWAYS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
CHANGE RD, P1=0	AUT_PACE	
GET PIN STATUS	AUT_PACE	
RESET RC. P1 aus der Menge {0, 1}	AUT_PACE	
VERIFY	AUT_PACE	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

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

[<=]

Hinweis (21) Kommandos, die gemäß [gemSpec_COS] mit einem Passwortobjekt arbeiten, sind: Activate, Change Reference Data, Deactivate, Delete, Disable Verification Requirement, Enable Verification Requirement, Get Pin Status, Reset Retry Counter, Verify, Terminate.

Card-G2-A_3286 - K_Personalisierung: Personalisierte Attribute von MF / PIN.CH

Bei der Personalisierung von PIN.CH MÜSSEN die in Tab_HBA_ObjSys_097 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 17: Tab_HBA_ObjSys_097 Personalisierte Attribute von MF / PIN.CH

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

[<=]

5.3.10 MF / PrK.HPC.AUTR_CVC.E256

PrK.HPC.AUTR_CVC.E256 ist der globale private Schlüssel für die Kryptographie mit elliptischen Kurven für C2C-Authentisierungen zwischen HBA/eGK und HBA/CMS, und zur Autorisierung der SMC-B. Der zugehörige öffentliche Schlüssel PuK.HPC.AUTR_CVC.E256 ist in C.HPC.AUTR_CVC.E256 (siehe Kapitel 5.3.9) enthalten.

Card-G2-A_2072 - K_Initialisierung: Initialisierte Attribute von MF / PrK.HPC.AUTR_CVC.E256

PrK.HPC.AUTR_CVC.E256 MUSS die in Tab_HBA_ObjSys_021 dargestellten Werte besitzen.

1034 **Tabelle 18: Tab_HBA_ObjSys_021 Initialisierte Attribute von MF /**
1035 **PrK.HPC.AUTR_CVC.E256**

Attribute	Wert	Bemerkung
Objektyp	privates Schlüsselobjekt, ELC 256	
keyIdentifier	'06' = 6	
privateElcKey	domainparameter = brainpoolP256r1	wird personalisiert
privateElcKey	keyData = AttributNotSet	
keyAvailable	Wildcard	
listAlgorithmIdentifier	alle Werte aus der Menge {elcRoleAuthentication}	
lifeCycleStatus	„Operational state (activated)“	
accessRuleSession keys	irrelevant	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERATE ASYMMETRIC KEY PAIR P1='81'	ALWAYS	
INTERNAL AUTHENTICATE	PWD(PIN.CH)	
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis 26:
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	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERATE ASYMMETRIC KEY	AUT_PACE	siehe Hinweis 26:

PAIR P1='81'		
INTERNAL AUTHENTICATE	AUT_PACE AND PWD(PIN.CH)	
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis 26:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	

[<=]

Hinweis (25) Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt ELC arbeiten, sind: Activate, Deactivate, Delete, External Authenticate, General Authenticate, Generate Asymmetric Key Pair, Internal Authenticate, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature, Terminate

Hinweis (26) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap. 5.9.

Card-G2-A_3288 - K_Personalisierung: Personalisierte Attribute von MF / PrK.HPC.AUTR_CVC.E256

Bei der Personalisierung von PrK.HPC.AUTR_CVC.E256 MÜSSEN die in Tab_HBA_ObjSys_099 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 19: Tab_HBA_ObjSys_099 Personalisierte Attribute von MF / PrK.HPC.AUTR_CVC.E256

Attribute	Wert	Bemerkung
keyAvailable	True	
privateElcKey	keyData = Wildcard	

[<=]

5.3.11 MF / PrK.HPC.AUTD_SUK_CVC.E256

PrK.HPC.AUTD_SUK_CVC.E256 ist der globale private Schlüssel für die Kryptographie mit elliptischen Kurven für C2C-Authentisierungen zwischen HBA/gSMC-KT und HBA/gSMC-K für die Übertragung von PIN-Daten und der DTBS zum HBA. Der zugehörige öffentliche Schlüssel PuK.HPC.AUTD_SUK_CVC.E256 ist in C.HPC.AUTD_SUK_CVC.E256 (siehe Kapitel 5.3.10) enthalten.

1061 **Card-G2-A_2075 - K_Initialisierung: Initialisierte Attribute von MF /**
 1062 **PrK.HPC.AUTD_SUK_CVC.E256**
 1063 PrK.HPC.AUTD_SUK_CVC.E256 MUSS die in Tab_HBA_ObjSys_024 dargestellten Werte
 1064 besitzen.
 1065

1066 **Tabelle 20: Tab_HBA_ObjSys_024 Initialisierte Attribute von MF /**
 1067 **PrK.HPC.AUTD_SUK_CVC.E256**

Attribute	Wert	Bemerkung
Objekttyp	privates Schlüsselobjekt, ELC 256	
keyIdentifier	'09' = 9	
privateElcKey	domainparameter = brainpoolP256r1	
privateElcKey	keyData = AttributNotSet	wird personalisiert
keyAvailable	Wildcard	
listAlgorithmIdentifier	Ein Wert aus der Menge {elcSessionkey4SM, elcAsynchronAdmin}	
lifeCycleStatus	„Operational state (activated)“	
numberScenarion	0	
accessRuleSessionkeys	irrelevant	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERATE ASYMMETRIC KEY PAIR P1='81'	ALWAYS	
GENERAL AUTHENTICATE	ALWAYS	
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis 28:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung

alle	NEVER	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERATE ASYMMETRIC KEY PAIR P1='81'	AUT_PACE	
General Authenticate	ALWAYS	
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis 28:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	

[<=]

Hinweis (27) Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt ELC arbeiten, sind: Activate, Deactivate, Delete, External Authenticate, General Authenticate, Generate Asymmetric Key Pair, Internal Authenticate, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature, Terminate

Hinweis (28) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap. 5.9.

Der zu PrK.HPC.AUTD_SUK_CVC.E256 (mit CVC-Inhaberprofil 53) gehörende öffentliche Schlüssel ist im Zertifikat C.HPC. AUTD_SUK_CVC.E256 enthalten.

Card-G2-A_3289 - K_Personalisierung: Personalisierte Attribute von MF / PrK.HPC.AUTD_SUK_CVC.E256

Bei der Personalisierung von PrK.HPC.AUTD_SUK_CVC.E256 MÜSSEN die in Tab_HBA_ObjSys_101 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 21: Tab_HBA_ObjSys_101 Personalisierte Attribute von MF / PrK.HPC.AUTD_SUK_CVC.E256

Attribute	Wert	Bemerkung
keyAvailable	True	

<i>privateElcKey</i>	keyData = Wildcard	
----------------------	--------------------	--

[<=]

5.3.12 Sicherheitsanker zum Import von CV-Zertifikaten

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

5.3.12.1 MF / PuK.RCA.CS.E256

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

Card-G2-A_2078-02 ~~Card-G2-A_2078-01~~ - K_Initialisierung: Initialisierte Attribute von MF / PuK.RCA.CS.E256

PuK.RCA.CS.E256 MUSS die in Tab_HBA_ObjSys_027 dargestellten Werte besitzen.

Tabelle 22: Tab_HBA_ObjSys_027 Initialisierte Attribute von MF / PuK.RCA.CS.E256

Attribute	Wert	Bemerkung
Objekttyp	öffentliches ELC Signaturprüfobjekt	
Für Echtkarten MÜSSEN die vier folgenden Attribute mit den unten angegebenen Werten initialisiert werden. Für Option_Erstellung_von_Testkarten MÜSSEN die vier folgenden Attribute mit Wildcard oder AttributeNotSet initialisiert werden.		
<i>keyIdentifier</i>	E 256 Root-CA-Kennung (5 Bytes) Erweiterung (3 Bytes)	
<i>expirationDate</i>	Jahr Monat Tag im Format YYMMDD gemäß [gemSpec_PKI#6.7.2.6], Wert gemäß [gemSpec_CVC_Root#5.4.2]	
CHAT	OID _{flags} = oid_cvc_fl_ti flagList = 'FF 0084 2006 00E3'	siehe Hinweis (32÷)
<i>publicKey</i>	Öffentlicher Schlüssel mit Domainparameter = brainpoolP256r1 gemäß [gemSpec_PKI#6.7.2.3] und gemäß [gemSpec_CVC_TSP[gemSpec_CVC_TSP#4.5]	

Für Echtkarten MÜSSEN die nachfolgenden Attribute mit den unten angegebenen Werten initialisiert werden.

Für Option_Erstellung_von_Testkarten MÜSSEN die nachfolgenden Attribute entweder mit den unten angegebenen Werten oder mit Wildcard oder AttributeNotSet initialisiert werden.

<i>oid</i>	ecdsa-with-SHA256 '2A8648CE3D040302' = {1.2.840.10045.4.3.2}	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
<i>accessRulesPublicSignatureVerificationObject</i>	Für alle relevanten Interfaces und alle relevanten Werte von lifeCycleStatus gilt: Delete → ALWAYS AUT_CMS OR AUT_CUP PSO Verify Certificate → ALWAYS	siehe Hinweis (31)
<i>accessRulesPublicAuthenticationObject</i>	Für alle relevanten Interfaces und alle relevanten Werte von lifeCycleStatus gilt: Delete → ALWAYS External Authenticate → ALWAYS	siehe Hinweis 31

Zugriffsregeln für die Kontaktschnittstelle

Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet

Zugriffsart	Zugriffsbedingung	Bemerkung
PSO Verify Cert.	ALWAYS	
Delete	AUT_CMS OR AUT_CUP	siehe Hinweis (31)
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	

Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)

Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
PSO Verify Cert.	ALWAYS	
Delete	AUT_CMS OR AUT_CUP	siehe Hinweis (31÷)
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	

[<=]

Hinweis (31) Das Kommando ist nur vom Inhaber des CMS- /CUP-Schlüssels ausführbar, siehe Kap. 5.9.

Hinweis (32) Während gemäß den Tabellen in [gemSpec_PKI] als RFU gekennzeichnete Bits einer Flaglisten in CV-Zertifikaten der Generation 2 auf ,0' zu setzen sind, werden RFU Bits einer Flagliste im CHAT eines Sicherheitsankers auf ,1' gesetzt.

Card-G2-A_3327-01 - K_Personalisierung: Personalisierte Attribute von MF / PuK.RCA.CS.E256 für Testkarten

Bei der Personalisierung von PuK.RCA.CS.E256 für Testkarten MÜSSEN die in Tab_HBA_ObjSys_153 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Wenn die restlichen Attribute von PuK.RCA.CS.E256 mit Wildcard oder AttributeNotSet initialisiert wurden, MÜSSEN sie gemäß den Vorgaben in der Initialisierungstabelle Tab_HBA_ObjSys_027 personalisiert werden.

Tabelle 23: Tab_HBA_ObjSys_153 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]
keyIdentifizier	E 256 Root-CA-Kennung (5 Bytes) Erweiterung (3 Bytes); Wert gemäß	

	keyIdentifier des personalisierten Schlüssels	
CHAT	<ul style="list-style-type: none"> OID_{flags} = oid_cvc_fl_ti flagList = 'FF 0084 2006 00E3' 	
expirationDate	Jahr Monat Tag im Format YYMMDD gemäß [gemSpec_PKI#6.7.2.6], Wert gemäß CXD des personalisierten Schlüssels	

[<=]

5.3.13 Asymmetrische Kartenadministration

Die hier beschriebene Variante der Administration des HBA betrifft ein Administrationssystem (i.A. ein Kartenmanagementsystem (CMS)) zur Administration des HBA.

Die Administration eines HBA 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 5.3.17 beschrieben.

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

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

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

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

Card-G2-A_3016-01 - K_Initialisierung: Initialisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256

PuK.RCA.ADMINCMS.CS.E256 MUSS die in Tab_HBA_ObjSys_082 dargestellten Attribute besitzen.

1157 **Tabelle 24: Tab_HBA_ObjSys_082 Initialisierte Attribute von MF /**
1158 **PuK.RCA.ADMINCMS.CS.E256**

Attribute	Wert	Bemerkung
Objektyp	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	<ul style="list-style-type: none"> OID_{flags} = oid_cvc_fl_cms flagList = 'FF BFFF FFFF FFFF' 	siehe Hinweis 34:
expirationDate	Identisch zu „expirationDate“ von PuK.RCS.CS.E256	
Für Echtkarten MÜSSEN die nachfolgenden Attribute mit den unten angegebenen Werten initialisiert werden. Für Option_Erstellung_von_Testkarten MÜSSEN die nachfolgenden Attribute entweder mit den unten angegebenen Werten oder mit Wildcard oder AttributeNotSet initialisiert werden.		
keyIdentifier	'0000 0000 0000 0013'	
lifeCycleStatus	„Operational state (activated)“	
publicKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Domainparameter = brainpoolP256r1	wird personalisiert
oid	ecdsa-with-SHA256 '2A8648CE3D040302' = {1.2.840.10045.4.3.2}	
accessRulesPublicSignatureVerificationObject	Für alle relevanten Interfacesarten und alle relevanten Werte von lifeCycleStatus gilt: Delete → AUT_CMS OR AUT_CUP PSO Verify Certificate → ALWAYS	
accessRulesPublicAuthenticationObject	Für alle relevanten Interfaces und alle	

	relevanten Werte von lifeCycleStatus gilt: Delete → ALWAYS	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsart	Zugriffsbedingung	Bemerkung
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
PSO Verify Certificate	ALWAYS	
Delete	AUT_CMS OR AUT_CUP	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktbehaftet		
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet		
alle	NEVER	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
PSO Verify Certificate	ALWAYS	
Delete	AUT_CMS OR AUT_CUP	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
alle	NEVER	

1159
1160

[<=]

1161 *Hinweis (33) Kommandos, die gemäß [gemSpec_COS] mit einem öffentlichen*
1162 *Signaturprüfobjekt arbeiten, sind: Activate, Deactivate, Delete, PSO Verify Certificate,*
1163 *Terminate*

1164 *Hinweis (34) Während gemäß den Tabellen in [gemSpec_COS]#H.4] als RFU*
1165 *gekennzeichnete Bits einer Flaglisten in CV-Zertifikaten der Generation 2 auf ,0' zu*

setzen sind, werden RFU Bits einer Flagliste im CHAT eines Sicherheitsankers auf „1“ gesetzt.

Card-G2-A_3290 - K_Personalisierung: Personalisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256

Bei der Personalisierung von PuK.RCA.ADMINCMS.CS.E256 MÜSSEN die in Tab_HBA_ObjSys_103 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Wenn die restlichen Attribute von PuK.RCA.ADMINCMS.CS.E256 mit Wildcard oder AttributeNotSet initialisiert wurden, MÜSSEN sie gemäß den Vorgaben in der Initialisierungstabelle Tab_HBA_ObjSys_082 personalisiert werden.

Tabelle 25: Tab_HBA_ObjSys_103 Personalisierte Attribute von MF / PuK.RCA.ADMINCMS.CS.E256

Attribute	Wert	Bemerkung
publicKey	Domainparameter = brainpoolP256r1 gemäß [gemSpec_PKI#6.7.2.3]	
publicKey Option_Erstellung _von_Testkarten	Domainparameter = brainpoolP256r1 gemäß [gemSpec_PKI#6.7.2.3] aus Test- Admin-CVC-Root	
CHAT	<ul style="list-style-type: none"> OID_{flags} = oid_cvc_fl_cms flagList = 'FF BFFF FFFF FFFF'	
expirationDate Option_Erstellung _von_Testkarten	Identisch zu „expirationDate“ des personalisierten PuK.RCA.CS.E256	

[<=]

5.3.14 Symmetrische Kartenadministration

Die hier beschriebene Variante der Administration des HBA betrifft ein Administrationssystem (i.A. ein Kartenmanagementsystem (CMS)) zur Administration des HBA.

Die Administration eines HBA 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 5.3.16 beschrieben.

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

Wenn die symmetrischen Schlüssel (SK.CMS und SK.CUP) für die Authentifizierung des Kartenadministrationssystems genutzt werden, dann MÜSSEN sie kartenindividuell personalisiert werden, so dass mit einem Schlüssel eines administrierenden Systems genau ein HBA administriert werden kann.

1198 Die Objekte müssen bei der Initialisierung angelegt werden. Bei der Personalisierung sind
1199 nur die Schlüssel zu personalisieren, die tatsächlich benötigt werden.

1200 5.3.14.1 MF / SK.CMS.AES128

1201 SK.CMS.AES128 (optional) ist der geheime AES-Schlüssel mit 128 bit Schlüssellänge für
1202 die Durchführung des HBA/CMS-Authentisierungsverfahrens mit Aufbau eines Trusted
1203 Channel.

1204 [Card-G2-A 2080-02](#) ~~Card-G2-A 2080-01~~ - K_Initialisierung: Initialisierte 1205 Attribute von MF / SK.CMS.AES128

1206 SK.CMS.AES128 MUSS die in Tab_HBA_ObjSys_029 dargestellten Werte besitzen.

1207 **Tabelle 26: Tab_HBA_ObjSys_029 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)“	
accessRuleSessionkeys	irrelevant	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
Mutual Authenticate	ALWAYS	
Mutual Authenticate General Authenticate	ALWAYS	

Delete	AUT_CMS OR AUT_CUP	siehe Hinweis (36÷)
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	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
Mutual <u>Authenticate</u> <u>General</u> Authenticate	ALWAYS	
Delete	AUT_CMS OR AUT_CUP	siehe Hinweis (36÷)
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	

[<=]

Hinweis (35) Kommandos, die gemäß [gemSpec_COS] mit einem symmetrischen Authentisierungsobjekt arbeiten, sind:

Activate, Deactivate, Delete, External Authenticate, General Authenticate, Get Security Status Key, Internal Authenticate, Mutual Authenticate, Terminate.

Hinweis (36) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap. 5.9.

Card-G2-A_3291 - 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_HBA_ObjSys_104 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

1223 **Tabelle 27: Tab_HBA_ObjSys_104 Personalisierte Attribute von MF / SK.CMS.AES128**

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

1224 [\leq]

1225 5.3.14.2 MF / SK.CMS.AES256

1226 SK.CMS.AES256 (optional) ist der geheime AES-Schlüssel mit 256 bit Schlüssellänge für
1227 die Durchführung des HBA/CMS-Authentisierungsverfahrens mit Aufbau eines Trusted
1228 Channel.

1229 Card-G2-A_2081-02~~Card-G2-A_2081-01~~ - K_Initialisierung: Initialisierte 1230 Attribute von MF / SK.CMS.AES256

1231 SK.CMS.AES256 MUSS die in Tab_HBA_ObjSys_030 dargestellten Werte besitzen.

1232 **Tabelle 28: Tab_HBA_ObjSys_030 Initialisierte Attribute von MF / SK.CMS.AES256**

Attribute	Wert	Bemerkung
Objektyp	Symmetrisches Authentisierungsobjekt	
<i>keyType</i>	AES-256	
<i>keyIdentifier</i>	'18' = 24	
<i>encKey</i>	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 256 Bit	wird personalisiert
<i>macKey</i>	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 256 Bit	wird personalisiert
<i>numberScenario</i>	0	
<i>algorithmIdentifier</i>	aesSessionkey4SM, siehe [gemSpec_COS]	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
accessRuleSessionkeys	irrelevant	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		

Zugriffsart	Zugriffsbedingung	Bemerkung
Mutual Authenticate	ALWAYS	
Mutual Authenticate General Authenticate	ALWAYS	
Delete	AUT_CMS OR AUT_CUP	siehe Hinweis (36+)
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	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
Mutual Authenticate General Authenticate	ALWAYS	
Delete	AUT_CMS OR AUT_CUP	siehe Hinweis (36+)
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	

[<=]

Card-G2-A_3292 - 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_HBA_ObjSys_105 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 29: Tab_HBA_ObjSys_105 Personalisierte Attribute von MF / SK.CMS.AES256

Attribute	Wert	Bemerkung
-----------	------	-----------

<i>encKey</i>	Symmetrischer Schlüssel AES.256 gemäß [gemSpec_Krypt#2.4]	
<i>macKey</i>	Symmetrischer Schlüssel AES.256 gemäß [gemSpec_Krypt#2.4]	

1242 [\leq]

1243 5.3.14.3 MF / SK.CUP.AES128

1244 Dieser AES-Schlüssel mit 128 bit Schlüssellänge wird benötigt, um dem CUPS
1245 administrative Zugriffe auf den HBA bezüglich der Zertifikate zu erlauben.

1246
1247
1248 **Card-G2-A 3293-02** ~~Card-G2-A 3293-01~~ - K_Initialisierung: Initialisierte
1249 **Attribute von MF / SK.CUP.AES128**
1250 SK.CUP.AES128 MUSS die in Tab_HBA_ObjSys_147 dargestellten Initialisierten Attribute
1251 besitzen.

1252 **Tabelle 30: Tab_HBA_ObjSys_147 Initialisierte Attribute von MF / SK.CUP.AES128**

Attribute	Wert	Bemerkung
Objektyp	Symmetrisches Authentisierungsobjekt	
<i>keyType</i>	AES-128	
<i>keyIdentifier</i>	'03' = 3	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
<i>encKey</i>	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 128 Bit	wird personalisiert
<i>macKey</i>	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 128 Bit	wird personalisiert
<i>numberScenario</i>	0	
<i>algorithmIdentifier</i>	aesSessionkey4SM, siehe [gemSpec_COS]	
<i>accessRuleSessionkeys</i>	irrelevant	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung

Mutual Authenticate	ALWAYS	
Mutual Authenticate General Authenticate	ALWAYS	
Delete	AUT_CMS OR AUT_CUP	siehe Hinweis (36÷)
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	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
Mutual Authenticate General Authenticate	ALWAYS	
Delete	AUT_CMS OR AUT_CUP	siehe Hinweis (36÷)
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	

[<=]

Card-G2-A_3294 - 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_HBA_ObjSys_148 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 31: Tab_HBA_ObjSys_148 Personalisierte Attribute von MF / SK.CUP.AES128

Attribute	Wert	Bemerkung
-----------	------	-----------

<i>encKey</i>	Symmetrischer Schlüssel AES.128 gemäß [gemSpec_Krypt#2.4]	
<i>macKey</i>	Symmetrischer Schlüssel AES.128 gemäß [gemSpec_Krypt#2.4]	

1263

1264 [\leq]

1265 5.3.14.4 MF / SK.CUP.AES256

1266 Dieser AES-Schlüssel mit 256 bit Schlüssellänge wird benötigt, um dem CUPS
1267 administrative Zugriffe auf den HBA bezüglich der Zertifikate zu erlauben.

1268 [Card-G2-A_3295-02](#) ~~Card-G2-A_3295-01~~ - K_Initialisierung: Initialisierte
1269 **Attribute von MF / SK.CUP.AES256**

1270 SK.CUP.AES256 MUSS die in Tab_HBA_ObjSys_149 dargestellten Initialisierten Attribute
1271 besitzen.

1272 **Tabelle 32: Tab_HBA_ObjSys_149 Initialisierte Attribute von MF / SK.CUP.AES256**

Attribute	Wert	Bemerkung
Objektyp	Symmetrisches Authentisierungsobjekt	
<i>keyType</i>	AES-256	
<i>keyIdentifier</i>	'04' = 4	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
<i>encKey</i>	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 256 Bit	wird personalisiert
<i>macKey</i>	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen symmetrischen AES-Schlüssel mit 256 Bit	wird personalisiert
<i>numberScenario</i>	0	
<i>algorithmIdentifier</i>	aesSessionkey4SM, siehe [gemSpec_COS]	
<i>accessRuleSessionkeys</i>	irrelevant	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
Mutual-Authenticate	ALWAYS	

Mutual <u>Authenticate</u> General Authenticate	ALWAYS	
Delete	AUT_CMS OR AUT_CUP	siehe Hinweis (36÷)
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	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
Mutual <u>Authenticate</u> <u>General</u> Authenticate	ALWAYS	
Delete	AUT_CMS OR AUT_CUP	siehe Hinweis (36÷)
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	

{<=>}[<=]

Card-G2-A_3296 - 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_HBA_ObjSys_150 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 33: Tab_HBA_ObjSys_150 Personalisierte Attribute von MF / SK.CUP.AES256

Attribute	Wert	Bemerkung
-----------	------	-----------

<i>encKey</i>	Symmetrischer Schlüssel AES.256 gemäß [gemSpec_Krypt#2.4]	
<i>macKey</i>	Symmetrischer Schlüssel AES.256 gemäß [gemSpec_Krypt#2.4]	

1284

1285 [\leq]

1286 5.3.15 MF / SK.CAN (Option kontaktlose Schnittstelle)

1287 Das Schlüsselobjekt SK.CAN (Card Access Number) dient dazu, eine kontaktlose
1288 Kommunikationsschnittstelle zum HBA kryptographisch abzusichern.

1289 **Card-G2-A_2868 - K_Initialisierung: Initialisierte Attribute von MF / SK.CAN**

1290 Wird die kontaktlose Schnittstelle genutzt, dann MUSS SK.CAN vorhanden sein und die in
1291 Tab_HBA_ObjSys_076 dargestellten Attribute besitzen.
1292

1293 **Tabelle 34: Tab_HBA_ObjSys_076 Initialisierte Attribute von MF / SK.CAN**

Attribute	Wert	Bemerkung
Objekttyp	symmetrisches Kartenverbindungsobjekt	
<i>keyIdentifier</i>	'02' = 2	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
Can	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für ein Schlüsselobjekt SK.CAN	
<i>algorithmIdentifier</i>	id-PACE-ECDH-GM-AES-CBC-CMAC-128	
<i>accessRuleSessionkeys</i>	irrelevant	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERAL AUTHENTICATE	ALWAYS	
DELETE	AUT_CMS OR AUT_CUP	
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	
Zugriffsregeln für die kontaktlose Schnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
GENERAL AUTHENTICATE	ALWAYS	
DELETE	AUT_CMS OR AUT_CUP	
Andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
Alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
Alle	NEVER	

[<=]

Hinweis (37) Kommandos, die gemäß [gemSpec_COS] mit symmetrischen Kartenverbindungsobjekten arbeiten, sind: Activate; Deactivate; Delete, General Authenticate, Terminate.

Card-G2-A_3297 - K_Personalisierung: Personalisierte Attribute von MF / SK.CAN

Bei der Personalisierung von SK.CAN MÜSSEN die in Tab_HBA_ObjSys_106 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 35: Tab_HBA_ObjSys_106 Personalisierte Attribute von MF / SK.CAN

Attribute	Wert	Bemerkung
can	SK.CAN gemäß [gemSpec_CAN_TI]	siehe [Card-G2-A_2869]

[<=]

Card-G2-A_2869 - K_Personalisierung: Generierung der CAN bei Verwendung der optionalen kontaktlosen Schnittstelle des HBA

Bei Nutzung der optionalen kontaktlosen Schnittstelle des HBA MUSS die Personalisierung für das Attribut can von SK.CAN eine sechsstellige Ziffernfolge gemäß [gemSpec_CAN_TI] setzen.

[<=]

5.3.16 Sicherheitsumgebungen auf MF-Ebene

Auf MF-Ebene wird ausschließlich die Sicherheitsumgebung SE#1 (Default-SE) verwendet. Es ist möglich, z. B. für die entfernte PIN-Eingabe, in SE#1 einen Trusted Channel aufzubauen.

5.4 Die Heilberufsanwendung DF.HPA

5.4.1 Dateistruktur und Dateiinhalt

Die Abbildung Abb_HBA_ObjSys_002 zeigt die Dateistruktur von DF.HPA.

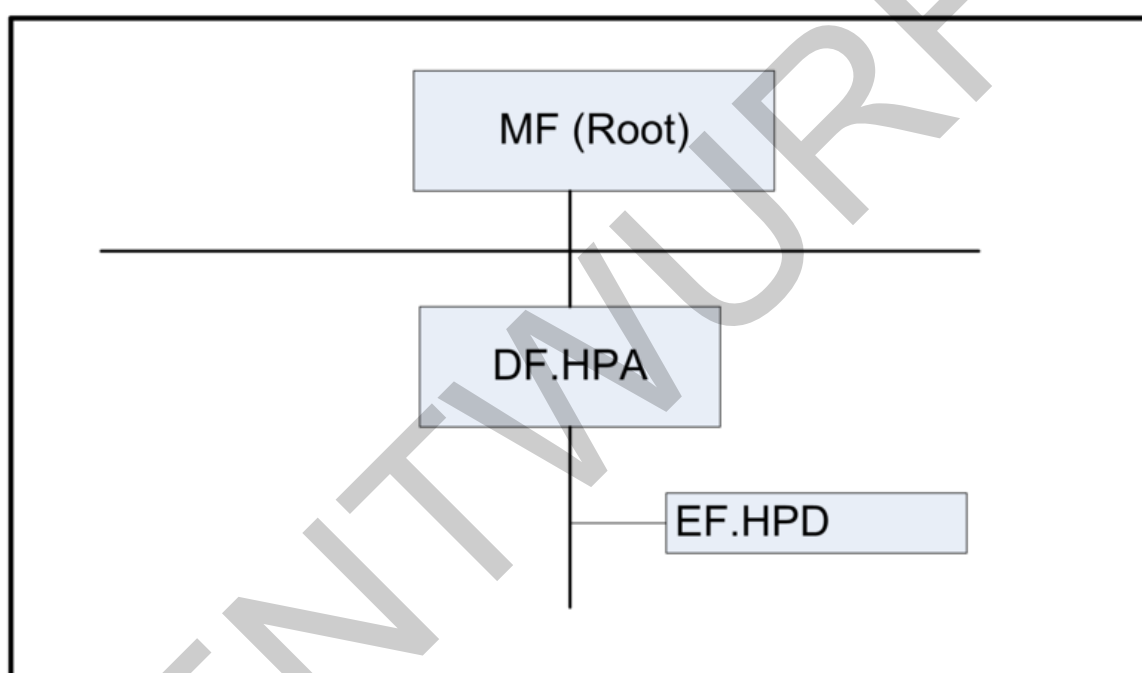


Abbildung 2: Abb_HBA_ObjSys_002 Dateistruktur von DF.HPA

5.4.2 MF / DF.HPA (Health Professional Application)

DF.HPA ist eine "Application" gemäß [gemSpec_COS#8.3.1.1], d. h. ist mittels Anwendungskennung selektierbar.

Card-G2-A_2082-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.HPA
DF.HPA MUSS die in Tab_HBA_ObjSys_031 dargestellten Werte besitzen.

Tabelle 36: Tab_HBA_ObjSys_031 Initialisierte Attribute von MF / DF.HPA

Attribute	Wert	Bemerkung
Objekttyp	Ordner	

<i>applicationIdentifier</i>	'D27600014602'	
<i>fileIdentifier</i>	–	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
<i>shareable</i>	True	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
GET RANDOM	ALWAYS	
LOAD APPLICATION (nach der HBA-Ausgabe)	AUT_CMS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	
Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
GET RANDOM	AUT_PACE	
LOAD APPLICATION (nach der HBA-Ausgabe)	AUT_CMS	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

- 1337
1338 [\leq]
1339 Hinweis (38) Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten,
1340 sind:
1341 Activate, Deactivate, Delete, Fingerprint, Get Random, List Public Key, Load Application,
1342 Select, Terminate DF.
1343 Schlüssel und CVCs für den Authentisierungsprozess befinden sich auf MF-Ebene. Die
1344 Heilberufsanwendung erlaubt das Anlegen weiterer Dateien, falls dafür in der Zukunft
1345 eine Notwendigkeit bestehen sollte, siehe Kapitel 5.9.

1346 5.4.2.1 MF / DF.HPA / EF.HPD (Health Professional Data)

1347 Das transparente Datei EF.HPD ist für die Speicherung von Daten vorgesehen, die sich
1348 auf den jeweiligen Heilberufler beziehen, z.B. die Bestätigung der Teilnahme an
1349 Fortbildungsmaßnahmen. Das File kann immer gelesen werden, aber eine Aktualisierung
1350 ist nur nach erfolgreicher Eingabe der PIN.CH möglich.

1351 Card-G2-A_2083 - K_Initialisierung: Initialisierte Attribute von MF / DF.HPA / 1352 EF.HPD

1353 EF.HPD MUSS die in Tab_HBA_ObjSys_032 dargestellten Werte besitzen.
1354

1355 **Tabelle 37: Tab_HBA_ObjSys_032 Initialisierte Attribute von MF / DF.HPA / EF.HPD**

Attribute	Wert	Bemerkung
Objektyp	transparentes Elementary File	
fileIdentifier	'D0 01'	
shortFileIdentifier	'01' = 1	
numberOfOctet	'08 00' Oktett = 2048 Oktett	
positionLogicalEndOfFile	'0'	
flagTransactionMode	True	
flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
body	kein Inhalt	wird später nachgeladen
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	ALWAYS	
ERASE BINARY SET LOGICAL EOF UPDATE BINARY WRITE BINARY	PWD(PIN.CH)	

andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	
Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
READ BINARY	AUT_PACE	
ERASE BINARY SET LOGICAL EOF UPDATE BINARY WRITE BINARY	AUT_PACE AND PWD(PIN.CH)	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

[<=]

Hinweis (39) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Set Logical Eof, Update Binary, Terminate, Write Binary.

5.4.2.2 Sicherheitsumgebungen

In DF.HPA wird das SE#1 verwendet.

5.5 Die Anwendung für die qualifizierte elektronische Signatur (DF.QES)

Dieses Kapitel enthält die Objekte, die die QES-Anwendung beschreiben. Dies ist gleichzeitig die Sicht einer Signaturanwendungskomponente, welche diese Anwendung nutzen möchte.

5.5.1 Dateistruktur und Dateinhalt

Die Abbildung Abb_HBA_ObjSys_003 zeigt die prinzipielle Dateistruktur der QES-Anwendung, die in Übereinstimmung mit [DIN66291-1] definiert ist.

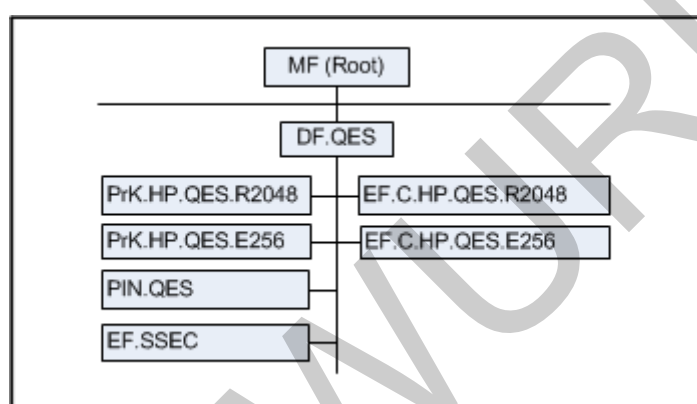


Abbildung 3 Abb_HBA_ObjSys_003 Prinzipielle Struktur der QES-Anwendung

Die QES-Anwendung beinhaltet EFs für die X.509-QES-Zertifikate für die Kryptographie mit RSA und mit elliptischen Kurven. Zusätzlich ist ein EF zur Anzeige des unterstützten Maximalwertes des SSEC angelegt.

5.5.2 MF / DF.QES (Qualified Electronic Signature Application)

DF.QES ist ein "Application Directory" gemäß [gemSpec_COS#8.3.1.1], d. h. ist mittels Anwendungskennung selektierbar.

Card-G2-A_2084-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.QES

DF.QES MUSS die in Tab_HBA_ObjSys_033 dargestellten Werte besitzen.

Tabelle 38: Tab_HBA_ObjSys_033 Initialisierte Attribute von MF / DF.QES

Attribute	Wert	Bemerkung
Objektyp	Ordner	
<i>applicationIdentifier</i>	'D276000066 01'	siehe Hinweis 40:
<i>fileIdentifier</i>	–	siehe Hinweis 41:

<i>lifeCycleStatus</i>	„Operational state (activated)“	
<i>shareable</i>	True	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
GET RANDOM	ALWAYS	
LOAD APPLICATION	AUT_CMS	Siehe Hinweis 43:
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	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
GET RANDOM	AUT_PACE	
LOAD APPLICATION	AUT_CMS	Siehe Hinweis 43:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

1388

1389 [\leq]

1390 Hinweis (40) Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten,
1391 sind:

1392 Activate, Deactivate, Delete, Fingerprint, Get Random, List Public Key, Load Application,
1393 Select, Terminate DF.

1394 Hinweis (41) Der Wert des Attributes applicationIdentifier ist in [ISO7816-4] festgelegt.

1395 Hinweis (42) herstellerspezifisch; Falls unterstützt, dann außerhalb des Intervalls ['1000',
1396 'FEFF']; siehe [ISO7816-4#8.1.1]

1397 Hinweis (43) Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe
1398 Kapitel 5.9.

1399 5.5.2.1 MF / DF.QES / PrK.HP.QES.R2048

1400 PrK.HP.QES.R2048 ist der private Schlüssel für die Kryptographie mit RSA zur
1401 Berechnung von qualifizierten elektronischen Signaturen. Die Eigenschaften der PIN.QES
1402 werden in Kapitel 5.5.2.2 dargestellt. Der zugehörige öffentliche Schlüssel
1403 PuK.HP.QES.R2048 ist in C.HP.QES.R2048 (siehe Kapitel 5.5.2.4) enthalten.

1404 Card-G2-A_2085-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.QES 1405 / PrK.HP.QES.R2048

1406 PrK.HP.QES.R2048 MUSS die in Tab_HBA_ObjSys_034 dargestellten Werte besitzen.
1407

1408 **Tabelle 39: Tab_HBA_ObjSys_034 Initialisierte Attribute von MF / DF.QES /**
1409 **PrK.HP.QES.R2048**

Attribute	Wert	Bemerkung
Objekttyp	privates Schlüsselobjekt RSA 2048	
keyIdentifizier	'04' = 4	
privateKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Modulslänge 2048 Bit	wird personalisiert
keyAvailable	WildCard	
listAlgorithmIdentifizier	alle Werte aus der Menge { signPSS }	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart SE#1	Zugriffsbedingung	Bemerkung
Generate Asymmetric Key Pair P1='81'	ALWAYS	
PSO Comp Dig Sig	PWD(PIN.QES)	siehe Hinweis 48:
Delete	herstellerspezifisch	siehe Hinweis 46:
andere	NEVER	
Zugriffsart SE#2	Zugriffsbedingung	Bemerkung
PSO Comp Dig Sig	PWD(PIN.QES) AND SmMac(flagTI.55)	siehe Hinweis 47:

	AND SmCmdEnc AND SmRespEnc	
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	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
Zugriffsart SE#1	Zugriffsbedingung	Bemerkung
Generate Asymmetric Key Pair P1='81'	AUT_PACE	
PSO Compute Digital Signature	AUT_PACE AND PWD(PIN.QES)	siehe Hinweis 48:
Delete	herstellerspezifisch	siehe Hinweis 46:
andere	NEVER	
Zugriffsart SE#2	Zugriffsbedingung	Bemerkung
PSO Compute Digital Signature	PWD(PIN.QES) AND SmMac(flagTI.55) AND SmCmdEnc AND SmRespEnc	siehe Hinweis 47:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	

1410
1411
1412
1413
1414

[<=]

- 1415 *Hinweis (44) Kommandos, die gemäß [gemSpec_COS] mit einem privaten*
1416 *Schlüsselobjekt RSA arbeiten, sind:*
1417 *Activate, Deactivate, Delete, External Authenticate, Generate Asymmetric Key Pair,*
1418 *Internal Authenticate, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature,*
1419 *Terminate*
- 1420 *Hinweis (45) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar,*
1421 *siehe Kap. 5.9.*
- 1422 *Hinweis (46) Die konkrete Zugriffsregel muss durch den Objektsystemhersteller in*
1423 *Abstimmung mit einer Bestätigungsstelle gemäß EU-Verordnung Nr. 910/2014 (eIDAS)*
1424 *festgelegt werden.*
- 1425 *Hinweis (47) Modus für Stapel- und Komfortsignatur, siehe [TR-03114] und [TR-03115].*
1426 *Geräteauthentisierung von gSMC-K mit Profil 51 (SAK)*
- 1427 *Hinweis (48) Modus für Einzel- oder Stapelsignatur ohne Geräteauthentisierung gemäß*
1428 *PIN.QES Start Security Status Evaluation Counter.*
1429

- 1430 **Card-G2-A_3298 - K_Personalisierung: Personalisierte Attribute von MF /**
1431 **DF.QES / PrK.HP.QES.R2048**
1432 Bei der Personalisierung von PrK.HP.QES.R2048 MÜSSEN die in Tab_HBA_ObjSys_108
1433 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

1434

- 1435 **Tabelle 40: Tab_HBA_ObjSys_108 Personalisierte Attribute von MF / DF.QES /**
1436 **PrK.HP.QES.R2048**

Attribute	Wert	Bemerkung
privateKey	Moduluslänge 2048 Bit	wird personalisiert
keyAvailable	True	

- 1437 [**<=**]

1438 **5.5.2.2 MF / DF.QES / PIN.QES**

- 1439 PIN.QES ist eine DF-spezifische PIN, die zum Schutz des privaten Schlüssels für die
1440 qualifizierte elektronische Signatur des Heilberufers (PrK.HP.QES.R2048) gemäß EU-
1441 Verordnung Nr. 910/2014 (eIDAS) verwendet wird.
- 1442 Die Nutzung des Rücksetz-Codes (Personal Unblocking Key, PUK) wird durch einen
1443 Nutzungszähler *pukUsage* beschränkt. Der Sicherheitsstatus von PIN.QES kann nur für
1444 eine begrenzte Anzahl von Signaturen verwendet werden, d. h. der SSEC-Maximalwert ist
1445 endlich.
- 1446 Die PIN-Referenz für die Kommandos Verify, Change Reference Data und Reset Retry
1447 Counter und andere PIN-Eigenschaften sind in der folgenden Tabelle
1448 Tab_HBA_ObjSys_037 zusammengefasst.

- 1449 **Card-G2-A_2088-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.QES**
1450 **/ PIN.QES**

- 1451 PIN.QES MUSS die in Tab_HBA_ObjSys_037 dargestellten Werte besitzen.

1452

- 1453 **Tabelle 41: Tab_HBA_ObjSys_037 Initialisierte Attribute von MF / DF.QES / PIN.QES**

Attribute	Wert	Bemerkung
-----------	------	-----------

Objekttyp	Passwortobjekt	
<i>pwdIdentifier</i>	'01' = 1	
<i>secret</i>	undefiniert	wird personalisiert
<i>minimumLength</i>	6	
<i>maximumLength</i>	8	
<i>startRetryCounter</i>	3	
<i>retryCounter</i>	3	
<i>transportStatus</i>	Transport-PIN	
<i>flagEnabled</i>	True	
<i>Start Security Status Evaluation Counter</i>	SE # 1: $1 \leq \text{SSEC} \leq 250$ SE # 2: $1 \leq \text{SSEC} \leq 250$	Werte wie in EF.SSEC angezeigt
PUK	undefiniert	wird personalisiert
<i>pukUsage</i>	10	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart SE#1	Zugriffsbedingung	Bemerkung
Change RD, P1=0	ALWAYS	
Get Pin Status	ALWAYS	
Reset RC., P1=1	ALWAYS	
Verify	ALWAYS	
andere	NEVER	
Zugriffsart SE#2	Zugriffsbedingung	Bemerkung
Change RD, P1=0	SmMac(flagTI.54) AND SmCmdEnc	
Get Pin Status	SmMac(flagTI.55)	
Reset RC., P1=1	SmMac(flagTI.54) AND SmCmdEnc	
Verify	SmMac(flagTI.54) AND SmCmdEnc	
andere	NEVER	

Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	
Zugriffsregel für logischen LCS „Termination state“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
Zugriffsart SE#1	Zugriffsbedingung	Bemerkung
Change RD, P1=0	AUT_PACE	
Get Pin Status	AUT_PACE	
Reset RC., P1=1	AUT_PACE	
Verify	AUT_PACE	
andere	NEVER	
Zugriffsart SE#2	Zugriffsbedingung	Bemerkung
Change RD, P1=0	SmMac(flagTI.54) AND SmCmdEnc	
Get Pin Status	SmMac(flagTI.55)	
Reset RC., P1=1	SmMac(flagTI.54) AND SmCmdEnc	
Verify	SmMac(flagTI.54) AND SmCmdEnc	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

1454

1455 [\leq]

1456 *Hinweis (49) Kommandos, die gemäß [gemSpec_COS] mit einem Passwortobjekt*
 1457 *arbeiten, sind: Activate, Change Reference Data, Deactivate, Delete, Disable Verification*
 1458 *Requirement, Enable Verification Requirement, Get Pin Status, Reset Retry Counter,*
 1459 *Verify, Terminate.*

Card-G2-A_3299 - K_Personalisierung: Personalisierte Attribute von MF / DF.QES / PIN.QES

Bei der Personalisierung von PIN.QES MÜSSEN die in Tab_HBA_ObjSys_111 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 42: Tab_HBA_ObjSys_111 Personalisierte Attribute von MF / DF.QES / PIN.QES

Attribute	Wert	Bemerkung
<i>secret</i>	PIN-Wert gemäß [gemSpec_PINPUK_TI]	Transport-PIN
<i>secretLength</i>	5 Ziffern (<i>minimumLength</i> - 1)	Länge der Transport-PIN
<i>PUK</i>	PUK-Wert gemäß [gemSpec_PINPUK_TI]	
<i>PUKLength</i>	Anzahl Ziffern aus dem Intervall [8, 12]	

[<=]

5.5.2.3 MF / DF.QES / EF.SSEC

Die transparente Datei EF.SSEC zeigt die SSEC-Maximalwerte an, die für eine konkrete Anwendungsumgebung des HBA gemäß Evaluierung und Bestätigung des HBA als Sichere Signaturerstellungseinheit definiert wurden.

Card-G2-A_2089-01 Card-G2-A_2089 - K_Initialisierung: Initialisierte Attribute von MF / DF.QES / EF.SSEC

EF.SSEC MUSS die in Tab_HBA_ObjSys_038 dargestellten Werte besitzen.

Tabelle 43: Tab_HBA_ObjSys_038 Initialisierte Attribute von MF / DF.QES / EF.SSEC

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
<i>fileIdentifier</i>	'D0 05'	
<i>shortFileIdentifier</i>	'05' = 5	
<i>numberOfOctet</i>	'002E' Oktett = 46 Oktett	
<i>positionLogicalEndOfFile</i>	'002E' Oktett = 46 Oktett	
<i>flagTransactionMode</i>	False	

flagChecksum	True	
lifeCycleStatus	„Operational state (activated)“	
shareable	True	
body	Inhalt gemäß den Werten für Start SecurityStatus-Evaluation-Counter für SE#1 und für SE#2 in PIN.QES (siehe Card-G2-A 2090-01 siehe Kapitel 5.5.2.2)	siehe Kapitel 5.5.2.2
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart SE#1, SE#2	Zugriffsbedingung	Bemerkung
READ BINARY	ALWAYS	
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	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
Zugriffsart SE#1	Zugriffsbedingung	Bemerkung
READ BINARY	AUT_PACE	
andere	NEVER	
Zugriffsart SE#2	Zugriffsbedingung	Bemerkung
READ BINARY	AUT_PACE SmMac(flagTI.55) AND SmRspEnc	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

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

[<=]

Hinweis (51) 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.

Der Inhalt von EF.SSEC (siehe Tab_HBA_ObjSys_038) wird während der Initialisierung gespeichert. Die externe Signaturanwendungskomponente kann den Inhalt der Datei lesen, um die Größe des Signaturstapels zu optimieren. Die Angaben in EF.SSEC müssen den implementierten SSEC-Maximalwerten entsprechen.

Card-G2-A_2090-01 - K_Initialisierung: Inhalt von EF.SSEC

Der Inhalt von EF.SSEC MUSS die in Tab_HBA_ObjSys_039 dargestellten Werte besitzen.

Tabelle 44: Tab_HBA_ObjSys_039 Inhalt von EF.SSEC

Tag	Länge	Bedeutung					
'7B'	'2C'	Datenobjekte der Sicherheitsumgebung					
		Tag	Länge	Wert	Bedeutung		
		'80'	'01'	'01'	Sicherheitsumgebung: 1		
		'A4'	'11'	Authentication Template			
				Tag	Länge	Wert	Bedeutung
				'82'	'06'	'D27600006601'	DF-Name: DF.QES
				'83'	'01'	'81'	Schlüsselreferenz: PIN.QES
				'95'	'01'	'08'	Usage Qualifier: Benutzerauthentisierung
				'C0'	'01'	'xx'	SSEC-Maximalwert, z.B. 250
		Tag	Länge	Wert	Bedeutung		
		'80'	'01'	'02'	Sicherheitsumgebung: 2		
		'A4'	'11'	Authentication Template			
				Tag	Länge	Wert	Bedeutung
				'82'	'06'	'D27600006601'	DF-Name: PIN.QES
				'83'	'01'	'81'	Schlüsselreferenz: PIN.QES

				'95'	'01'	'08'	Usage Qualifier: Benutzerauthentisierung
				'C0'	'01'	'xx'	SSEC-Maximalwert, z.B. 250

1490

1491 [\leq]

1492 *Anmerkung 1 – Abgesehen vom SSEC-Object werden unterhalb des Tag '7B' die*
1493 *Datenobjekte gemäß [ISO7816-4] verwendet.*

1494 *Anmerkung 2 – Die SSEC-Maximalwerte im Bereich 251-254 sollten nicht verwendet*
1495 *werden, da diese Werte im COS möglicherweise eine andere Bedeutung haben. Falls ein*
1496 *unbegrenzter SSEC notwendig ist, muss das in EF.SSEC durch die Kodierung 'FF' im*
1497 *SSEC-Feld angezeigt werden.*

1498

1499 **5.5.2.4 MF / DF.QES / EF.C.HP.QES.R2048**

1500 Die transparente Datei EF.C.HP.QES.R2048 enthält das X.509-Zertifikat für die
1501 Kryptographie mit RSA mit dem öffentlichen Schlüssel des Heilberufers
1502 PuK.HP.QES.R2048 für die qualifizierte elektronische Signatur gemäß EU-Verordnung Nr.
1503 910/2014 (eIDAS). Das zugehörnde private Schlüsselobjekt PrK.HP.QES.R2048 ist im
1504 Kapitel 5.5.2.1 definiert.

1505 **Card-G2-A 2091-02 Card-G2-A 2091-01 - K_Initialisierung: Initialisierte** 1506 **Attribute von MF / DF.QES / EF.C.HP.QES.R2048**

1507 EF.C.HP.QES.R2048 MUSS die in Tab_HBA_ObjSys_040 dargestellten Werte besitzen.

1508 **Tabelle 45: Tab_HBA_ObjSys_040 Initialisierte Attribute von MF / DF.QES /**
1509 **EF.C.HP.QES.R2048**

Attribute	Wert	Bemerkung
Objektyp	transparentes Elementary File	
fileIdentifier	'C0 00'	
shortFileIdentifier	'10' = 16	
numberOfOctet	'07 6C' Oktett = 1900 Oktett	
positionLogicalEndOfFile	'0' Wildcard	siehe Card-G2-A 2673
flagTransactionMode	True	
flagChecksum	False	
lifeCycleStatus	„Operational state (activated)“	

shareable	True	
body	kein Inhalt	wird personalisiert
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart SE#1, SE#2	Zugriffsbedingung	Bemerkung
Delete	herstellerspezifisch	siehe Hinweis (53÷)
Read Binary	ALWAYS	
Erase Binary Set Logical EOF Update Binary Write Binary	herstellerspezifisch	siehe Hinweis (53÷)
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	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
Zugriffsart SE#1	Zugriffsbedingung	Bemerkung
Delete	herstellerspezifisch	siehe Hinweis (53÷)
Read Binary	AUT_PACE	
Erase Binary Set Logical EOF Update Binary Write Binary	herstellerspezifisch	siehe Hinweis (53÷)
andere	NEVER	
Zugriffsart SE#2	Zugriffsbedingung	Bemerkung
Delete	herstellerspezifisch	siehe Hinweis (53÷)

Read Binary	SmMac(flagTI.55) AND SmRspEnc	
Erase Binary Set Logical EOF Update Binary Write Binary	herstellerspezifisch	siehe Hinweis (53÷)
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

[<=]

Hinweis (52) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Set Logical Eof, Update Binary, Terminate, Write Binary.

Hinweis (53) Die konkrete Zugriffsregel muss durch den Objektsystemhersteller, der diese Option umsetzt, in Abstimmung mit einer Bestätigungsstelle gemäß EU-Verordnung Nr. 910/2014 (eIDAS) festgelegt werden.

Card-G2-A 3301-01 Card-G2-A-3301 - K_Personalisierung: Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES.R2048

Bei der Personalisierung von EF.C.HP.QES.R2048 MÜSSEN die in Tab_HBA_ObjSys_113 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 46: Tab_HBA_ObjSys_113 Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES.R2048

Attribute	Wert	Bemerkung
positionLogical EndOfFilepositionLogicalEndOfFile	Zahl der tatsächlich belegten OktetteWildcard	Zahl der tatsächlich belegten Oktette
body	C.HP.QES.R2048 gemäß [gemSpec_PKI#5.2] passend zu dem privaten Schlüssel in PrK.HP.QES.R2048	

[<=]

5.5.2.5 MF / DF.QES / PrK.HP.QES.E256

PrK.HP.QES.E256 ist der private Schlüssel für die Kryptographie mit elliptischen Kurven zur Berechnung von qualifizierten elektronischen Signaturen. Die Eigenschaften der PIN.QES werden in Kapitel 5.5.2.2 dargestellt. Der zugehörige öffentliche Schlüssel PuK.HP.QES.E256 ist in C.HP.QES.E256 (siehe Kapitel 5.5.2.7) enthalten.

Card-G2-A_3629-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.QES / PrK.HP.QES.E256

PrK.HP.QES.E256 MUSS die in Tab_HBA_ObjSys_160 dargestellten initialisierten Attribute besitzen.

Tabelle 47: Tab_HBA_ObjSys_160 Initialisierte Attribute MF / DF.QES / PrK.HP.QES.E256

Attribute	Wert	Bemerkung
Objektyp	privates Schlüsselobjekt, ELC 256	
keyIdentifier	'06' = 6	
lifeCycleStatus	„Operational state (activated)“	
privateElcKey	domainparameter = brainpoolP256r1	wird personalisiert
privateElcKey	keyData = AttributNotSet	
keyAvailable	Wildcard	
listAlgorithmIdentifier	alle Werte aus der Menge, [gemSpec_COS] {signECDSA}	
accessRuleSessionkeys	irrelevant	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart SE#1	Zugriffsbedingung	Bemerkung
Generate Asymmetric Key Pair P1='81'	ALWAYS	
PSO Comp Dig Sig	PWD(PIN.QES)	siehe Hinweis 48:
Delete	herstellerspezifisch	siehe Hinweis 46:
andere	NEVER	
Zugriffsart SE#2	Zugriffsbedingung	Bemerkung
PSO Comp Dig Sig	PWD(PIN.QES) AND SmMac(flagTI.55) AND SmCmdEnc AND SmRespEnc	siehe Hinweis 47:
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	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
Zugriffsart SE#1	Zugriffsbedingung	Bemerkung
Generate Asymmetric Key Pair P1='81'	AUT_PACE	
PSO Compute Digital Signature	AUT_PACE AND PWD(PIN.QES)	siehe Hinweis 48:
Delete	herstellerspezifisch	siehe Hinweis 46:
andere	NEVER	
Zugriffsart SE#2	Zugriffsbedingung	Bemerkung
PSO Compute Digital Signature	PWD(PIN.QES) AND SmMac(flagTI.55) AND SmCmdEnc AND SmRspEnc	siehe Hinweis 47:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	

[<=]

Card-G2-A_3630 - K_Personalisierung: Personalisierte Attribute von MF / DF.QES / PrK.HP.QES.E256

Bei der Personalisierung von PrK.HP.QES.E256 MÜSSEN die in Tab_HBA_ObjSys_161 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 48: Tab_HBA_ObjSys_161 Personalisierte Attribute von MF / DF.QES / PrK.HP.QES.E256

Attribute	Wert	Bemerkung
<i>keyAvailable</i>	true	
<i>privateElcKey</i>	keyData = Wildcard	

[<=]

5.5.2.6 MF / DF.QES / EF.C.HP.QES.E256

Die transparente Datei EF.C.HP.QES.E256 enthält das X.509-Zertifikat für die Kryptographie mit elliptischen Kurven mit dem öffentlichen Schlüssel des Heilberufers PuK.HP.QES.E256 für die qualifizierte elektronische Signatur gemäß EU-Verordnung Nr. 910/2014 (eIDAS). Das zugehörende private Schlüsselobjekt PrK.HP.QES.E256 ist im Kapitel 5.5.2.6 definiert.

Card-G2-A 3631-01 ~~Card-G2-A-3631~~ - K_Initialisierung: Initialisierte Attribute von MF / DF.QES / EF.C.HP.QES.E256

EF.C.HP.QES.E256 MUSS die in Tab_HBA_ObjSys_162 dargestellten initialisierten Attribute besitzen.

Tabelle 49: Tab_HBA_ObjSys_162 Initialisierte Attribute von MF / DF.QES / EF.C.HP.QES.E256

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
<i>fileIdentifier</i>	'C0 06'	
<i>shortFileIdentifier</i>	'06' = 6	
<i>numberOfOctet</i>	'0B B8' Oktett = 3000 Oktett	
<i>positionLogicalEndOfFile</i>	'0' Wildcard	wird personalisiert siehe Card-G2-A 2673
<i>flagTransactionMode</i>	True	
<i>flagChecksum</i>	False	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
<i>shareable</i>	True	
<i>body</i>	kein Inhalt	wird personalisiert
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart SE#1, SE#2	Zugriffsbedingung	Bemerkung
Delete	herstellerspezifisch	siehe Hinweis (53÷)
Read Binary	ALWAYS	

Erase Binary Set Logical EOF Update Binary Write Binary	herstellerspezifisch	siehe Hinweis (53÷)
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	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
Zugriffsart SE#1	Zugriffsbedingung	Bemerkung
Delete	herstellerspezifisch	siehe Hinweis (53÷)
Read Binary	AUT_PACE	
Erase Binary Set Logical EOF Update Binary Write Binary	herstellerspezifisch	siehe Hinweis (53÷)
andere	NEVER	
Zugriffsart SE#2	Zugriffsbedingung	Bemerkung
Delete	herstellerspezifisch	siehe Hinweis (53÷)
Read Binary	SmMac(flagTI.55) AND SmRspEnc	
Erase Binary Set Logical EOF Update Binary Write Binary	herstellerspezifisch	siehe Hinweis (53÷)
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung

alle	herstellerspezifisch	
------	----------------------	--

[<=][<=]

Hinweis (57) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Set Logical Eof, Update Binary, Terminate, Write Binary.

Card-G2-A 3632-01 Card-G2-A-3632 - K_Personalisierung: Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES.E256

Bei der Personalisierung von EF.C.HP.QES.E256 MÜSSEN die in Tab_HBA_ObjSys_163 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 64: Tab_HBA_ObjSys_163 Personalisierte Attribute von MF / DF.QES / EF.C.HP.QES.E256

Attribute	Wert	Bemerkung
positionLogical EndOfFile positionLogicalEndOfFile	Zahl der tatsächlich belegten Öktette Wildcard	siehe Card-G2-A_2673
body	C.HP.QES.E256 gemäß [gemSpec_PKI] passend zu dem privaten Schlüssel in PrK.HP.QES.E256	

[<=]

5.6 Die ESIGN-Anwendung (DF.ESIGN)

5.6.1 Dateistruktur und Dateinhalt

Die Abbildung Abb_HBA_ObjSys_004 zeigt die prinzipielle Struktur der ESIGN-Anwendung, die in Übereinstimmung mit [EN14890-1] definiert ist.

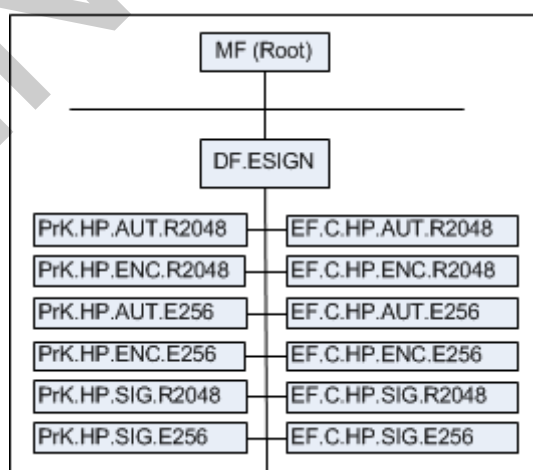


Abbildung 4: Abb_HBA_ObjSys_004 Prinzipielle Struktur von DF.ESIGN

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

DF.ESIGN ist ein "Application Directory" gemäß [gemSpec_COS#8.3.1.1], d. h. ist mittels Anwendungskennung selektierbar.

Die allgemeine ESIGN Anwendung ist in DF.ESIGN dargestellt und wird im HBA für folgende Funktionen genutzt:

- Die Client/Server-Authentisierung,
- die Nachrichtensignatur,
- die Schlüssel-Chiffrierungsfunktion für die kryptographische Sicherung von Daten.

Card-G2-A_2097-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN

DF.ESIGN MUSS die in Tab_HBA_ObjSys_045 dargestellten Werte besitzen.

Tabelle 50: Tab_HBA_ObjSys_045 Initialisierte Attribute von MF / DF.ESIGN

Attribute	Wert	Bemerkung
Objektyp	Ordner	
<i>applicationIdentifier</i>	'A000000167 455349474E'	siehe Hinweis 59:
<i>fileIdentifier</i>	–	siehe Hinweis 60:
<i>lifeCycleStatus</i>	„Operational state (activated)“	
<i>shareable</i>	True	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
GET RANDOM	ALWAYS	
LOAD APPLICATION	AUT_CMS	siehe Hinweis 62:
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	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		

Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
GET RANDOM	AUT_PACE	
LOAD APPLICATION	AUT_CMS	siehe Hinweis 62:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

[<=]

Hinweis (58) Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten, sind:

Activate, Deactivate, Delete, Fingerprint, Get Random, List Public Key, Load Application, Select, Terminate DF.

Hinweis (59) Der Wert des Attributes applicationIdentifier ist in [ISO7816-4] festgelegt.

Hinweis (60) herstellerspezifisch; Falls unterstützt, dann außerhalb des Intervalls ['1000', 'FEFF']; siehe [gemSpec_COS#8.1.1].

Hinweis (61) Da sich weder dieser Ordner noch darüberliegende Ebenen deaktivieren lassen, sind diese Zustände für Objekte im Kapitel 5.6 im Allgemeinen irrelevant.

Hinweis (62) Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe Kap. 5.9.

5.6.2.1 MF / DF.ESIGN / PrK.HP.AUT.R2048

PrK.HP.AUT.R2048 ist der private Schlüssel für die Kryptographie mit RSA für Client/Server-Authentisierung. Der zugehörige öffentliche Schlüssel PuK.HP.AUT.R2048 ist in C.HP.AUT.R2048 (siehe Kapitel 5.6.2.3) enthalten.

Card-G2-A_2098-02 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.AUT.R2048

PrK.HP.AUT.R2048 MUSS die in Tab_HBA_ObjSys_046 dargestellten Werte besitzen.

Tabelle 51: Tab_HBA_ObjSys_046 Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.AUT.R2048

Attribute	Wert	Bemerkung
Objektyp	privates Schlüsselobjekt, RSA 2048	

<i>keyIdentifier</i>	'02' = 2	
<i>privateKey</i>	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Modulslänge 2048 Bit	wird personalisiert
<i>keyAvailable</i>	Wildcard	
<i>listAlgorithmIdentifier</i>	alle Werte aus der Menge, siehe [gemSpec_COS] {rsaClientAuthentication, signPKCS1_V1_5, signPSS}	
<i>lifeCycleStatus</i>	„Operational state (activated)“	

Zugriffsregeln für die Kontaktschnittstelle

Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet

Zugriffsart	Zugriffsbedingung	Bemerkung
Internal Authenticate PSO Compute Digital Signature	PWD(PIN.CH)	Die Zugriffsregel für PIN.CH ist auf MF-Ebene definiert
Generate Asymmetric Key Pair P1='81'	ALWAYS	
Delete	AUT_CMS OR AUT_CUP	siehe Hinweis (67÷)
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	

Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)

Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos

Zugriffsart	Zugriffsbedingung	Bemerkung
Internal Authenticate PSO Compute Digital Signature	AUT_PACE AND PWD(PIN.CH)	Die Zugriffsregel für PIN.CH ist auf MF-Ebene definiert

Generate Asymmetric Key Pair P1='81'	AUT_CMS OR AUT_CUP OR AUT_PACE	
Delete	AUT_CMS OR AUT_CUP	siehe Hinweis (67÷)
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	

[<=]

Hinweis (66) Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt RSA arbeiten, sind:

Activate, Deactivate, Delete, External Authenticate, Generate Asymmetric Key Pair, Internal Authenticate, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature, Terminate

Hinweis (67) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap. 5.9.

Card-G2-A_3305 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.AUT.R2048

Bei der Personalisierung von PrK.HP.AUT.R2048 MÜSSEN die in Tab_HBA_ObjSys_118 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 52: Tab_HBA_ObjSys_118 Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.AUT.R2048

Attribute	Wert	Bemerkung
privateKey	Moduluslänge 2048 Bit	wird personalisiert
keyAvailable	True	

[<=]

5.6.2.2 MF / DF.ESIGN / PrK.HP.ENC.R2048

PrK.HP.ENC.R2048 ist der private Schlüssel für die Kryptographie mit RSA für das Entschlüsseln von Dokumenten-Chiffrierungsschlüsseln. Der zugehörige öffentliche Schlüssel PuK.HP.ENC.R2048 ist in C.HP.ENC.R2048 (siehe Kapitel 5.6.2.4) enthalten.

Card-G2-A 2101-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.ENC.R2048

PrK.HP.ENC.R2048 MUSS die in Tab_HBA_ObjSys_049 dargestellten Werte besitzen.

Tabelle 53: Tab_HBA_ObjSys_049 Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.ENC.R2048

Attribut	Wert	Bemerkung
Objekttyp	privates Schlüsselobjekt, RSA 2048	
keyIdentifier	'03' = 3	
privateKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Modulslänge 2048 Bit	wird personalisiert
keyAvailable	WildCard	
listAlgorithmIdentifier	alle Werte aus der Menge, siehe [gemSpec_COS] {rsaDecipherOaep}	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis (69)
PSO Decipher PSO Transcipher	PWD(PIN.CH)	Die Zugriffsregel für PIN.CH ist auf MF-Ebene definiert
GENERATE ASYMMETRIC KEY PAIR P1='81'	ALWAYS	
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	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis (69÷)
PSO Decipher PSO Transcipher	AUT_PACE AND PWD(PIN.CH)	Die Zugriffsregel für PIN.CH ist auf MF-Ebene definiert
GENERATE ASYMMETRIC KEY PAIR P1='81'	AUT_CMS OR AUT_CUP OR AUT_PACE	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	

[<=]

Hinweis (68) Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt RSA arbeiten, sind:

Activate, Deactivate, Delete, External Authenticate, Generate Asymmetric Key Pair, Internal Authenticate, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature, Terminate

Hinweis (69) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.9.

In Bezug auf die Schlüssellängen müssen dieselben Konventionen wie für die Schlüssel der qualifizierten elektronischen Signatur berücksichtigt werden, siehe [ALGCAT] und [TR-03116-1].

Card-G2-A_3306 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.ENC.R2048

Bei der Personalisierung von PrK.HP.ENC.R2048 MÜSSEN die in Tab_HBA_ObjSys_121 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 54: Tab_HBA_ObjSys_121 Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.ENC.R2048

Attribute	Wert	Bemerkung
<i>privateKey</i>	Moduluslänge 2048 Bit	wird personalisiert
<i>keyAvailable</i>	True	

[<=]

5.6.2.3 MF / DF.ESIGN / EF.C.HP.AUT.R2048

Die Datei EF.C.HP.AUT.R2048 enthält ein Zertifikat für die Kryptographie mit RSA mit dem öffentlichen Schlüssel PuK.HP.AUT.R2048. Das zugehörnde private Schlüsselobjekt PrK.HP.AUT.R2048 ist in Kapitel 5.6.2.1 definiert.

[Card-G2-A 2107-01](#) ~~Card-G2-A-2107~~ - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.AUT.R2048

EF.C.HP.AUT.R2048 MUSS die in Tab_HBA_ObjSys_055 dargestellten Werte besitzen.

Tabelle 55: Tab_HBA_ObjSys_055 Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.AUT.R2048

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
<i>fileIdentifier</i>	'C5 00'	
<i>shortFileIdentifier</i>	'01' = 1	
<i>numberOfOctet</i>	'07 6C' Oktett = 1900 Oktett	
<i>positionLogicalEndOfFile</i>	'0' Wildcard	siehe Card-G2-A 2673
<i>flagTransactionMode</i>	True	
<i>flagChecksum</i>	False	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
<i>shareable</i>	True	
<i>body</i>	kein Inhalt	wird personalisiert
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE	AUT_CMS-OR-AUT_CUP	siehe Hinweis 71:

READ BINARY	ALWAYS	
DELETE SET LOGICAL EOF WRITE BINARY	AUT_CMS OR AUT_CUP	siehe Hinweis (71÷)
andere READ BINARY	ALWAYS 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	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
DELETE SET LOGICAL EOF WRITE BINARY	AUT_CMS OR AUT_CUP	siehe Hinweis (71÷)
READ BINARY	AUT_PACE OR AUT_CMS OR AUT_CUP OR AUT_CUPPACE	
SET LOGICAL EOF WRITE BINARY	AUT_CMS OR AUT_CUP	siehe Hinweis 71÷
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

1676
1677
1678

[<=]

Hinweis (70) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Set Logical Eof, Update Binary, Terminate, Write Binary.

Hinweis (71) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.9.

Card-G2-A 3307-01 ~~Card-G2-A-3307~~ - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.AUT.R2048

Bei der Personalisierung von EF.C.HP.AUT.R2048 MÜSSEN die in Tab_HBA_ObjSys_127 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 56: Tab_HBA_ObjSys_127 Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.AUT.R2048

Attribute	Wert	Bemerkung
<i>positionLogicalEndOfFile</i>	Zahl der tatsächlich belegten Oktette <u>Wildcard</u>	<u>siehe Card-G2-A 2673</u>
<i>body</i>	C.HP.AUT.R2048 gemäß [gemSpec_PKI#5.2] passend zu dem privaten Schlüssel in PrK.HP.AUT.R2048	

[<=]

5.6.2.4 MF / DF.ESIGN / EF.C.HP.ENC.R2048

Die Datei EF.C.HP.ENC.R2048 enthält ein Zertifikat für die Kryptographie mit RSA mit dem öffentlichen Schlüssel PuK.HP.ENC.R2048. Das zugehörige private Schlüsselobjekt PrK.HP.ENC.R2048 ist im Kapitel 5.6.2.2 definiert.

Card-G2-A 2110-02 ~~Card-G2-A-2110-01~~ - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.ENC.R2048

EF.C.HP.ENC.R2048 MUSS die in Tab_HBA_ObjSys_056 dargestellten Werte besitzen.

Tabelle 57: Tab_HBA_ObjSys_056 Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.ENC.R2048

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
<i>fileIdentifier</i>	'C2 00'	
<i>shortFileIdentifier</i>	'02' = 2	
<i>numberOfOctet</i>	'07 6C' Oktett = 1900 Oktett	
<i>positionLogicalEndOfFile</i>	'0' <u>Wildcard</u>	<u>wird personalisiert</u> <u>siehe Card-G2-A 2673</u>
<i>flagTransactionMode</i>	True	

<i>flagChecksum</i>	False	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
<i>shareable</i>	True	
<i>body</i>	kein Inhalt	wird personalisiert
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
Delete	AUT_CMS OR AUT_CUP	siehe Hinweis 73:
Read Binary	ALWAYS	
Delete Set Logical EOF Write Binary	AUT_CMS OR AUT_CUP	siehe Hinweis (73:)
andereRead Binary	ALWAYS 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	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
Delete Set Logical EOF Write Binary	AUT_CMS OR AUT_CUP	siehe Hinweis (73:)
Read Binary	AUT_PACE OR AUT_CMS OR AUT_CUP OR AUT_PACE	
Set Logical EOF Write Binary	AUT_CMS OR AUT_CUP	siehe Hinweis 73:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		

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

[<=]

Hinweis (72) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Set Logical Eof, Update Binary, Terminate, Write Binary.

Hinweis (73) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.9.

Card-G2-A 3308-01 Card-G2-A-3308 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.ENC.R2048

Bei der Personalisierung von EF.C.HP.ENC.R2048 MÜSSEN die in Tab_HBA_ObjSys_129 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 58: Tab_HBA_ObjSys_129 Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.ENC.R2048

Attribute	Wert	Bemerkung
positionLogicalEndOfFile	Zahl der tatsächlich belegten Oktette Wildcard	siehe Card-G2-A 2673
body	C.HP.ENC.R2048 gemäß [gemSpec_PKI#5.2] passend zu dem privaten Schlüssel in PrK.HP.ENC.R2048	

[<=]

5.6.2.5 MF / DF.ESIGN / PrK.HP.AUT.E256

PrK.HP.AUT.E256 ist der private Schlüssel für die Kryptographie mit elliptischen Kurven für Client/Server-Authentisierung. Der zugehörige öffentliche Schlüssel PuK.HP.AUT.E256 ist in C.HP.AUT.E256 (siehe Kapitel 5.6.2.7) enthalten.

Card-G2-A 3639-02 Card-G2-A-3639-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.AUT.E256

PrK.HP.AUT.E256 MUSS die in Tab_HBA_ObjSys_170 dargestellten initialisierten Attribute besitzen.

Tabelle 59: Tab_HBA_ObjSys_170 Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.AUT.E256

Attribute	Wert	Bemerkung
Objektyp	privates Schlüsselobjekt, ELC 256	
keyIdentifier	'06' = 6	

lifeCycleStatus	„Operational state (activated)“	
privateElcKey	domainparameter = brainpoolP256r1	wird personalisiert
privateElcKey	keyData = AttributNotSet	
keyAvailable	Wildcard	
listAlgorithmIdentifier	alle Werte aus der Menge, [gemSpec_COS] {signECDSA}	
accessRuleSessionkeys	irrelevant	

Zugriffsregeln für die Kontaktschnittstelle

Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet

Zugriffsart	Zugriffsbedingung	Bemerkung
PSO Compute Digital Signature	PWD(PIN.CH)	
Generate Asymmetric Key Pair P1='81'	ALWAYS	
Delete	AUT_CMS OR AUT_CUP	siehe Hinweis (75÷)
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	

Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)

Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos

Zugriffsart	Zugriffsbedingung	Bemerkung
PSO Compute Digital Signature	AUT_PACE AND PWD(PIN.CH)	

Generate Asymmetric Key Pair P1='81'	AUT_CMS OR AUT_CUP OR AUT_PACE	
Delete	AUT_CMS OR AUT_CUP	siehe Hinweis (75÷)
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	

[<=]

Hinweis (74) Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt RSA arbeiten, sind:

Activate, Deactivate, Delete, External Authenticate, Generate Asymmetric Key Pair, Internal Authenticate, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature, Terminate

Hinweis (75) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kap. 5.9.

Card-G2-A_3640 - K_Personalisierung: Personalisierte MF / DF.ESIGN / PrK.HP.AUT.E256

Bei der Personalisierung von PrK.HP.AUT.E256 MÜSSEN die in Tab_HBA_ObjSys_171 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 60: Tab_HBA_ObjSys_171 Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.AUT.E256

Attribute	Wert	Bemerkung
keyAvailable	true	
privateElcKey	keyData = Wildcard	

[<=]

5.6.2.6 MF / DF.ESIGN / PrK.HP.ENC.E256

PrK.HP.ENC.E256 ist der private Schlüssel für die Kryptographie mit elliptischen Kurven für das Entschlüsseln von Dokumenten-Chiffrierungsschlüsseln. Der zugehörige öffentliche Schlüssel PuK.HP.ENC.E256 ist in C.HP.ENC.E256 (siehe Kapitel 5.6.2.8) enthalten.

Card-G2-A 3641-02 ~~Card-G2-A-3641-01~~ - K_Initialisierung: Initialisierte
Attribute von MF / DF.ESIGN / PrK.HP.ENC.E256

PrK.HP.ENC.E256 MUSS die in Tab_HBA_ObjSys_172 dargestellten initialisierten Attribute besitzen.

Tabelle 61: Tab_HBA_ObjSys_172 Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.ENC.E256

Attribute	Wert	Bemerkung
Objekttyp	privates Schlüsselobjekt, ELC 256	
keyIdentifier	'05' = 5	
lifeCycleStatus	„Operational state (activated)“	
privateElcKey	domainparameter = brainpoolP256r1	wird personalisiert
privateElcKey	keyData = AttributNotSet	
keyAvailable	Wildcard	
listAlgorithmIdentifier	alle Werte aus der Menge, [gemSpec_COS] {elcSharedSecretCalculation}	
accessRuleSessionkeys	irrelevant	

Zugriffsregeln für die Kontaktschnittstelle

Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet

Zugriffsart	Zugriffsbedingung	Bemerkung
Delete	AUT_CMS OR AUT_CUP	siehe Hinweis (77÷)
PSO Decipher PSO Transcipher	PWD(PIN.CH)	Die Zugriffsregel für PIN.CH ist auf MF-Ebene definiert
Generate Asymmetric Key Pair P1='81'	ALWAYS	

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	

Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)

Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos

Zugriffsart	Zugriffsbedingung	Bemerkung
Delete	AUT_CMS OR AUT_CUP	siehe Hinweis (77÷)
PSO Decipher PSO Transcipher	AUT_PACE AND PWD(PIN.CH)	Die Zugriffsregel für PIN.CH ist auf MF-Ebene definiert
Generate Asymmetric Key Pair P1='81'	AUT_CMS OR AUT_CUP OR AUT_PACE	
andere	NEVER	

Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos

Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	

[<=]

Hinweis (76) Kommandos, die gemäß [gemSpec_COS] mit einem privaten Schlüsselobjekt RSA arbeiten, sind:

Activate, Deactivate, Delete, External Authenticate, Generate Asymmetric Key Pair, Internal Authenticate, PSO Decipher, PSO Transcipher, PSO Compute Digital Signature, Terminate

Hinweis (77) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.9.

Card-G2-A_3642 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.ENC.E256

Bei der Personalisierung von PrK.HP.ENC.E256 MÜSSEN die in Tab_HBA_ObjSys_173 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

1769 **Tabelle 62: Tab_HBA_ObjSys_173 Personalisierte Attribute von MF / DF.ESIGN /**
1770 **PrK.HP.ENC.E256**

Attribute	Wert	Bemerkung
<i>keyAvailable</i>	true	
<i>privateElcKey</i>	keyData = Wildcard	

1771
1772 [**<=**]

1773 **5.6.2.7 MF / DF.ESIGN / EF.C.HP.AUT.E256**

1774 Die Datei EF.C.HP.AUT.E256 enthält ein Zertifikat für die Kryptographie mit elliptischen
1775 Kurven mit dem öffentlichen Schlüssel PuK.HP.AUT.E256. Das zugehörige private
1776 Schlüsselobjekt PrK.HP.AUT.E256 ist in Kapitel 5.6.2.5 definiert.

1777 **Card-G2-A 3643-01Card-G2-A-3643 - K_Initialisierung: Initialisierte Attribute** 1778 **von MF / DF.ESIGN / EF.C.HP.AUT.E256**

1779 EF.C.HP.AUT.E256 MUSS die in Tab_HBA_ObjSys_174 dargestellten initialisierten
1780 Attribute besitzen.

1781 **Tabelle 63: Tab_HBA_ObjSys_174 Initialisierte Attribute von MF / DF.ESIGN /**
1782 **EF.C.HP.AUT.E256**

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
<i>fileIdentifier</i>	'C5 06'	
<i>shortFileIdentifier</i>	'06' = 6	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
<i>flagTransactionMode</i>	True	
<i>flagChecksum</i>	False	
<i>numberOfOctet</i>	'0B B8' Oktett = 3000 Oktett	
<i>positionLogicalEndOfFile</i>	'0' <u>Wildcard</u>	wird personalisiertsiehe Card-G2-A 2673
<i>shareable</i>	True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifisch	
<i>body</i>	kein Inhalt	wird personalisiert
Zugriffsregeln für die Kontaktschnittstelle		

Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet

Zugriffsart	Zugriffsbedingung	Bemerkung
Delete Set Logical EOF Write Binary	AUT_CMS OR AUT_CUP	siehe Hinweis (79÷)
Read Binary	ALWAYS	
Set Logical EOF Write Binary	AUT_CMS OR AUT_CUP	siehe Hinweis 79÷
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	

Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)

Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos

Zugriffsart	Zugriffsbedingung	Bemerkung
Delete Set Logical EOF Write Binary	AUT_CMS OR AUT_CUP	siehe Hinweis (79÷)
Read Binary	AUT_PAGE OR AUT_CMS OR AUT_CUP OR AUT_PAGE	
Set Logical EOF Write Binary	AUT_CMS OR AUT_CUP	siehe Hinweis 79÷
andere	NEVER	

Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos

Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

Zugriffsregel für logischen LCS „Termination state“ kontaktlos

Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

[<=]

Hinweis (78) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Set Logical Eof, Update Binary, Terminate, Write Binary.

Hinweis (79) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.9.

Card-G2-A 3644-01 ~~Card-G2-A-3644~~ - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.AUT.E256

Bei der Initialisierung von EF.C.HP.AUT.E256 MÜSSEN die in Tab_HBA_ObjSys_175 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 64: Tab_HBA_ObjSys_175 Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.AUT.E256

Attribute	Wert	Bemerkung
positionLogicalEndOfFile	Zahl der tatsächlich belegten OktetteWildcard	siehe Card-G2-A 2673
body	C.HP.AUT.E256 gemäß [gemSpec_PKI] passend zu dem privaten Schlüssel in PrK.HP.AUT.E256	

[<=]

5.6.2.8 MF / DF.ESIGN/ EF.C.HP.ENC.E256

Die Datei EF.C.HP.ENC.E256 enthält ein Zertifikat für die Kryptographie mit elliptischen Kurven mit dem öffentlichen Schlüssel PuK.HP.ENC.E256. Das zugehörige private Schlüsselobjekt PrK.HP.ENC.E256 ist im Kapitel 5.6.2.6 definiert.

Card-G2-A 3645-01 ~~Card-G2-A-3645~~ - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.ENC.E256

EF.C.HP.ENC.E256 MUSS die in Tab_HBA_ObjSys_176 dargestellten initialisierten Attribute besitzen.

Tabelle 65: Tab_HBA_ObjSys_176 Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.ENC.E256

Attribute	Wert	Bemerkung
Objektyp	transparentes Elementary File	
fileIdentifier	'C2 05' C2 05'	
shortFileIdentifier	'05' 05' = 5	
lifeCycleStatus	'Operational state (activated)'	
flagTransactionMode	True	

flagChecksum	False	
numberOfOctet	'0B B8' Oktett'0B B8' Oktette = 3000 OktettOktette	
positionLogicalEndOfFile	'0'Wildcard	wird personalisiertsiehe Card-G2-A 2673
shareable	True, falls Option_logische_Kanäle vorhanden ist, sonst herstellerspezifischTrue	
body	kein Inhalt	wird personalisiert

Zugriffsregeln für die Kontaktschnittstelle

ZugriffsregelZugriffsregeln für die Kontaktschnittstelle, für den logischen LCS „Operational state (activated)“ kontaktbehaftet)

Zugriffsart	Zugriffsbedingung	Bemerkung
Delete	AUT_CMS OR AUT_CUP	siehe Hinweis 81÷
Read Binary	ALWAYS	
Delete Set Logical EOF Write Binary	AUT_CMS OR AUT_CUP	siehe Hinweis (81÷)
andereRead Binary	ALWAYSNEVER	

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	

Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden), für den logischen LCS "Operational state (activated)“

Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos

Zugriffsart	Zugriffsbedingung	Bemerkung
Delete Set Logical EOF Write Binary	AUT_CMS OR AUT_CUP	siehe Hinweis (81÷)
Read Binary	AUT_PACE OR AUT_CMS OR AUT_CUP OR AUT_PACE	

Set Logical EOF Write Binary	AUT_CMS OR AUT_CUP	siehe Hinweis 81:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

[<=]

Hinweis (80) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Set Logical Eof, Update Binary, Terminate, Write Binary.

Hinweis (81) Das Kommando ist nur vom Inhaber des CMS- / CUP-Schlüssels ausführbar, siehe Kapitel 5.9.

Card-G2-A 3646-01 Card-G2-A-3646 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.ENC.E256

Bei der Initialisierung von EF.C.HP.ENC.E256 MÜSSEN die in Tab_HBA_ObjSys_177 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 66: Tab_HBA_ObjSys_177 Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.ENC.E256

Attribute	Wert	Bemerkung
positionLogicalEndOfFile	Zahl der tatsächlich belegten Oktette Wildcard	siehe Card-G2-A 2673
body	C.HP.ENC.E256 gemäß [gemSpec_PKI] passend zu dem privaten Schlüssel in PrK.HP.ENC.E256	

[<=]

5.6.2.9 MF / DF.ESIGN / EF.C.HP.SIG.R2048

Dieses EF enthält das Zertifikat zum Schlüssel PrK.HP.SIG.R2048.

A 15220-01A-15220 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.SIG.R2048

EF.C.HP.SIG.R2048 MUSS die in Tab_HBA_ObjSys_130 dargestellten Werte besitzen.

Tabelle 67: Tab_HBA_ObjSys_130 initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.SIG.R2048

Attribute	Wert	Bemerkung
-----------	------	-----------

Objekttyp	transparentes Elementary File	
<i>fileIdentifier</i>	'C0 00'	
<i>shortFileIdentifier</i>	'10' = 16	
<i>numberOfOctet</i>	'0B B8' Oktett = 3000 Oktett	
<i>positionLogicalEndOfFile</i>	0Wildcard	siehe Card-G2-A 2673
<i>flagTransactionMode</i>	True	
<i>flagChecksum</i>	False	
<i>lifeCycleStatus</i>	"Operational state (activated)"	
<i>shareable</i>	True	
<i>body</i>	kein Inhalt	
Zugriffsregeln für die Kontaktschnittstelle, für den logischen LCS "Operational state (activated)"		
Zugriffsart	Zugriffsbedingung	
DELETE SET LOGICAL EOF WRITE BINARY	AUT_CMS OR AUT_CUP	
READ BINARY	ALWAYS	
Zugriffsregeln für die kontaktlose Schnittstelle, für den logischen LCS "Operational state (activated)"		
DELETE SET LOGICAL EOF WRITE BINARY	AUT_CMS OR AUT_CUP	
READ BINARY	AUT_PAGE OR AUT_CMS OR AUT_CUP OR AUT_PAGE	

[{<=>}\[<=\]](#)

A 15221-01A-15221 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.SIG.R2048

Bei der Personalisierung von EF.C.HP.SIG.R2048 MÜSSEN die in Tab_HBA_ObjSys_136 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 68: Tab_HBA_ObjSys_136 Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.SIG.R2048

Attribute	Wert	Bemerkung
<i>positionLogicalEndOfFile</i>	Zahl der tatsächlich belegten Oktette Wildcard	siehe Card-G2-A 2673
<i>body</i>	C.HP.SIG.R2048 gemäß [gemSpec_PKI] passend zu dem privaten Schlüssel in PrK.HP.SIG.R2048	

[<=]

5.6.2.10 MF / DF.ESIGN / EF.C.HP.SIG.E256

Dieses EF enthält das Zertifikat zum Schlüssel PrK.HP.SIG.E256.

A 15222-01A-15222 - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.SIG.E256

EF.C.HP.SIG.E256 MUSS die in Tab_HBA_ObjSys_131 dargestellten Werte besitzen.

Tabelle 69: Tab_HBA_ObjSys_131 Initialisierte Attribute von MF / DF.ESIGN / EF.C.HP.SIG.E256

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
<i>fileIdentifier</i>	'C0 07'	
<i>shortFileIdentifier</i>	'07' = 7	
<i>numberOfOctet</i>	'0B B8' Oktett = 3000 Oktett	
<i>positionLogicalEndOfFile</i>	0 Wildcard	siehe Card-G2-A 2673
<i>flagTransactionMode</i>	True	
<i>flagChecksum</i>	False	
<i>lifeCycleStatus</i>	"Operational state (activated)"	

shareable	True	
body	kein Inhalt	
Zugriffsregeln für die Kontaktschnittstelle, für den logischen LCS "Operational state (activated)"		
Zugriffsart	Zugriffsbedingung	
DELETE SET LOIGCAL EOF WRITE BINARY	AUT_CMS OR AUT_CUP	
READ BINARY	ALWAYS	
Zugriffsregeln für die kontaktlose Schnittstelle, für den logischen LCS "Operational state (activated)"		
Zugriffsart	Zugriffsbedingung	
DELETE SET LOIGCAL EOF WRITE BINARY	AUT_CMS OR AUT_CUP	
READ BINARY	AUT_PAGE OR AUT_CMS OR AUT_CUP OR AUT_PACE	

[\[<=>\]\[<=\]](#)

A_15223-01A-15223 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.SIG.E256

Bei der Personalisierung von EF.C.HP.SIG.E256 MÜSSEN die in Tab_HBA_ObjSys_137 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 70: Tab_HBA_ObjSys_137 Personalisierte Attribute von MF / DF.ESIGN / EF.C.HP.SIG.E256

Attribute	Wert	Bemerkung
positionLogicalEndOfFile	Zahl der tatsächlich belegten OktetteWildcard	siehe Card-G2-A 2673
body	C.HP.SIG.E2048 gemäß [gemSpec_PKI] passend zu dem privaten Schlüssel in PrK.HP.SIG.E2048	

[\[<=\]](#)

5.6.2.11 MF / DF.ESIGN / PrK.HP.SIG.R2048

Dieses Objekt enthält den privaten Signaturschlüssel für RSA-Signaturen.

[A_15224-01A-15224](#) - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.SIG.R2048

PrK.HP.SIG.R2048 MUSS die in Tab_HBA_ObjSys_132 dargestellten Werte besitzen.

Tabelle 71: Tab_HBA_ObjSys_132 Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.SIG.R2048

Attribute	Wert	Bemerkung
Objektyp	privates Schlüsselobjekt, RSA 2048	
keyIdentifier	'04' = 4	
lifeCycleStatus	"Operational state (activated)"	
privateKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Moduluslänge 2048 Bit	
keyAvailable	Wildcard	
listAlgorithmIdentifier	alle Werte aus der Menge, [gemSpec_COS] {signPSS}	
Zugriffsregeln für die Kontaktschnittstelle, für den logischen LCS "Operational state (activated)"		
Zugriffsart	Zugriffsbedingung	
PSO Compute Digital Signature	PWD(PIN.CH)	
GENERATE ASYMMETRIC KEY PAIR (P1='81')	ALWAYS	
DELETE	AUT_CMS OR AUT_CUP	
Zugriffsregeln für die kontaktlose Schnittstelle, für den logischen LCS "Operational state (activated)"		
Zugriffsart	Zugriffsbedingung	
PSO Compute Digital Signature	AUT_PACE AND PWD(PIN.CH)	
GENERATE ASYMMETRIC KEY PAIR (P1='81')	AUT_CMS OR AUT_CUP OR AUT_PACE	

DELETE	AUT_CMS OR AUT_CUP	
--------	--------------------	--

[\[<=>\]](#) [\[<=\]](#)

A_15225 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.SIG.R2048

Bei der Personalisierung von PrK.HP.SIG.R2048 MÜSSEN die in Tab_HBA_ObjSys_133 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 72: Tab_HBA_ObjSys_133 Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.SIG.R2048E256

Attribute	Wert	Bemerkung
<i>privateKey</i>	Moduluslänge 2048 Bit	
<i>keyAvailable</i>	True	

[<=]

5.6.2.12 MF / DF.ESIGN / PrK.HP.SIG.E256

Dieses Objekt enthält den privaten Signaturschlüssel für ECC-Signaturen.

[A_15226-01A_15226](#) - K_Initialisierung: Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.SIG.E256

PrK.HP.SIG.E256 MUSS die in Tab_HBA_ObjSys_134 dargestellten Werte besitzen.

Tabelle 73: Tab_HBA_ObjSys_134 Initialisierte Attribute von MF / DF.ESIGN / PrK.HP.SIG.E256

Attribute	Wert	Bemerkung
Objekttyp	privates Schlüsselobjekt, ELC 256	
<i>keyIdentifier</i>	'07' = 7	
<i>lifeCycleStatus</i>	"Operational state (activated)"	
<i>privateElcKey</i>	<ul style="list-style-type: none"> <i>domainparameter</i> = brainpoolP256r1 <i>keyData</i> = AttributeNotSet 	
<i>keyAvailable</i>	Wildcard	

<i>listAlgorithmIdentifizier</i>	alle Werte aus der Menge, [gemSpec_COS] {signECDSA}	
Zugriffsregeln für die Kontaktschnittstelle, für den logischen LCS "Operational state (activated)"		
Zugriffsart	Zugriffsbedingung	
PSO Compute Digital Signature	PWD(PIN.CH)	
GENERATE ASYMMETRIC KEY PAIR (P1='81')	ALWAYS	
DELETE	AUT_CMS OR AUT_CUP	
Zugriffsregeln für die kontaktlose Schnittstelle, für den logischen LCS "Operational state (activated)"		
Zugriffsart	Zugriffsbedingung	
PSO Compute Digital Signature	AUT_PACE AND PWD(PIN.CH)	
GENERATE ASYMMETRIC KEY PAIR (P1='81')	<u>AUT_CMS OR AUT_CUP OR AUT_PACE</u>	
DELETE	AUT_CMS OR AUT_CUP	

[<=]

A_15227 - K_Personalisierung: Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.SIG.E256

Bei der Personalisierung von PrK.HP.SIG.E256 MÜSSEN die in Tab_HBA_ObjSys_135 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 74: Tab_HBA_ObjSys_135 Personalisierte Attribute von MF / DF.ESIGN / PrK.HP.SIG.E256

Attribute	Wert	Bemerkung
<i>keyAvailable</i>	True	
<i>privateElcKey</i>	keyData = WildCard	

[<=]

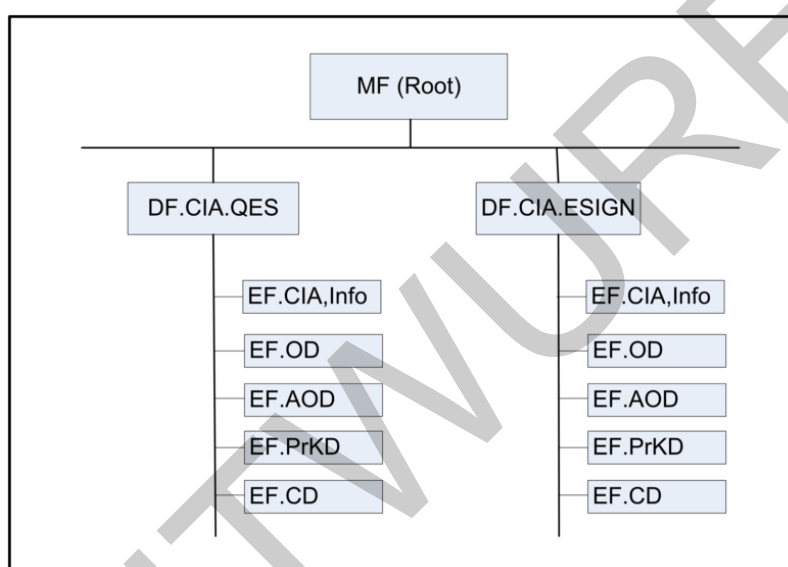
5.6.3 Sicherheitsumgebungen

DF.ESIGN wird ausschließlich in SE#1 (Default SE) genutzt. Es ist möglich, in SE#1 einen Trusted Channel aufzubauen, um beispielsweise Remote-Konfigurationen mit einem stationären HBA zu ermöglichen.

1899 5.7 Die kryptographischen Informationsanwendungen

1900 In [EN14890-1] ist das Vorhandensein einer kryptographischen Informationsanwendung
1901 (CIA) vorgeschrieben, um unterstützte Algorithmen, Dateikennungen etc. anzuzeigen,
1902 welche für die entsprechende QES- bzw. ESIGN-Anwendung relevant sind. Das jeweilige
1903 DF.CIA.x enthält dazu die Dateien Cryptographic Information Application (CIAInfo),
1904 Object Directory (OD), Authentication Object Directory (AOD), Private Key Directory
1905 (PrKD) und Certificate Directory (CD). Die verwendeten Objektattribute und die
1906 Dateiinhalte sind konform zu [ISO7816-15] und [ISO8825-1].

1907 Die Abbildung Abb_HBA_ObjSys_005 zeigt die prinzipielle Struktur der kryptographischen
1908 Informationsanwendungen (CIAs), die mit der QES- und der ESIGN-Anwendung
1909 verknüpft sind.



1910
1911 **Abbildung 5: Abb_HBA_ObjSys_005 DF.CIA-Anwendungen und ihre Unterstrukturen**

1912 5.7.1 MF / DF.CIA.QES (Cryptographic Information Applications)

1913 **Card-G2-A_2117-01 - K_Initialisierung: Initialisierte Attribute von MF /**
1914 **DF.CIA.QES**

1915 DF.CIA.QES MUSS die in Tab_HBA_ObjSys_057 dargestellten Werte besitzen.

1916
1917 **Tabelle 75: Tab_HBA_ObjSys_057 Initialisierte Attribute von MF / DF.CIA.QES**

Attribute	Wert	Bemerkung
Objektyp	Ordner	
<i>applicationIdentifier</i>	"E828BD080F D27600006601"	siehe Hinweis 82:
<i>fileIdentifier</i>	–	siehe Hinweis 83:
<i>lifeCycleStatus</i>	„Operational state (activated)“	
<i>shareable</i>	True	
Zugriffsregeln für die Kontaktschnittstelle		

Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
GET RANDOM	ALWAYS	
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	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
GET RANDOM	AUT_PACE	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

[<=]

5.7.1.1 MF / DF.CIA.QES / EF.CIA.CIAInfo

Card-G2-A 2119-02 ~~Card-G2-A-2119-01~~ - K_Initialisierung: Initialisierte Attribute von MF / DF.CIA.QES / EF.CIA.CIAInfo

MF / DF.CIA.QES / EF.CIA.CIAInfo MUSS die in Tab_HBA_ObjSys_059 dargestellten Werte besitzen.

Tabelle 76: Tab_HBA_ObjSys_059 Initialisierte Attribute von MF / DF.CIA.QES / EF.CIA.CIAInfo (Cryptographic Information Application Info)

Attribute	Wert	Bemerkung
Objektyp	transparentes Elementary File	

<i>fileIdentifier</i>	'50 32'	siehe Hinweis (83÷)
<i>shortFileIdentifier</i>	'12'= 18	siehe Hinweis (83÷)
<i>numberOfOctet</i>	' 00 A5' Oktett = 165 Oktett	
<i>positionLogicalEndOfFile</i>	' 00 A5' Oktett = 165 Oktett numberOfOctet	
<i>flagTransactionMode</i>	False	
<i>flagChecksum</i>	True	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
<i>shareable</i>	True	
<i>body</i>	30 81 A2 02 01 01 80 1F 51 75 61 6C 69 66 69 65 64 20 53 69 67 6E 61 74 75 72 65 20 41 70 70 6E 69 63 61 74 69 6F 6E 03 02 05 60 30 0D 30 0B 02 01 01 04 06 D2 76 00 00 66 01 A2 69 30 49 02 01 01 02 01 43 30 2F A0 0F 30 0D 06 09 60 86 48 01 65 03 04 02 01 05 00 A1 1C 30 1A 06 09 2A 86 48 86 F7 0D 01 01 08 30 0D 06 09 60 86 48 01 65 03 04 02 01 05 00 03 02 06 40 06 09 2A 86 48 86 F7 0D 01 01 0A 02 01 05 30 1C 02 01 02 02 04 80 00 00 05 05 00 03 02 06 40	

06 08 2A 86 48 CE 3D 04 03 02 02 01 00siehe unterhalb dieser Tabelle		
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
Read Binary	ALWAYS	
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	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
Read Binary	AUT_PACE	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

```

1928  [<=]30 81a2
1929  | 02 01 01
1930  | 80 1f 5175616c6966696564205369676e6174757265204170706c6963617469666e
1931  | 03 02 0560
1932  | 30 0d
1933  | | 30 0b
1934  | | | 02 01 01
1935  | | | 04 06 d27600006601
1936  | a2 69
1937  | | 30 49
1938  | | | 02 01 01
1939  | | | 02 01 43
1940

```

1941 | | | 30 2f
1942 | | | | a0 0f
1943 | | | | | 30 0d
1944 | | | | | | 06 09 608648016503040201
1945 | | | | | | 05 00
1946 | | | | a1 1c
1947 | | | | | 30 1a
1948 | | | | | | 06 09 2a864886f70d010108
1949 | | | | | | 30 0d
1950 | | | | | | | 06 09 608648016503040201
1951 | | | | | | | 05 00
1952 | | | 03 02 0640
1953 | | | 06 09 2a864886f70d01010a
1954 | | | 02 01 05
1955 | | 30 1c
1956 | | | 02 01 02
1957 | | | 02 04 80000005
1958 | | | 05 00
1959 | | | 03 02 0640
1960 | | | 06 08 2a8648ce3d040302
1961 | | | 02 01 00[<=]

1962 *Hinweis (82) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF*
1963 *arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Set*
1964 *Logical Eof, Update Binary, Terminate, Write Binary.*

1965 *Hinweis (83) Die Werte der Attribute fileIdentifier und shortFileIdentifier sind in in*
1966 *[ISO7816-15] festgelegt.*

1967 5.7.1.2 MF / DF.CIA.QES / EF.OD

1968 ~~Card-G2-A 2120-02~~Card-G2-A-2120-01 - K_Initialisierung: Initialisierte
1969 **Attribute von MF / DF.CIA.QES / EF.OD (Object Directory)**

1970 MF / DF.CIA.QES / EF.OD MUSS die in Tab_HBA_ObjSys_060 dargestellten Werte
1971 besitzen.

1972 **Tabelle 77: Tab_HBA_ObjSys_060 Initialisierte Attribute von MF / DF.CIA.QES / EF.OD**

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	'50 31'	siehe Hinweis (85÷)
shortFileIdentifier	'11' = 17	siehe Hinweis (85÷)
numberOfOctet	'00 18' Oktett = 24 Oktett	
positionLogicalEndOfFile	'00 18' Oktett = 24 Oktett <u>numberOfOctet</u>	
flagTransactionMode	False	

flagChecksum	True	
lifeCycleStatus	Operational state (activated)	
shareable	True	
body	A8-06 30-04 04-02-50-34 A0-06 30-04 04-02-50-35 A4-06 30-04 04-02-50-38	siehe unterhalb dieser Tabelle

Zugriffsregeln für die Kontaktschnittstelle

Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet

Zugriffsart	Zugriffsbedingung	Bemerkung
Read Binary	ALWAYS	
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	

Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)

Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos

Zugriffsart	Zugriffsbedingung	Bemerkung
Read Binary	AUT_PACE	
andere	NEVER	

Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos

Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

Zugriffsregel für logischen LCS „Termination state“ kontaktlos

Zugriffsart	Zugriffsbedingung	Bemerkung
-------------	-------------------	-----------

alle	herstellerspezifisch	
------	----------------------	--

[<=] a8 06

| 30 04

| | 04 02 5034

a0 06

| 30 04

| | 04 02 5035

a4 06

| 30 04

| | 04 02 5038 **[<=]**

Hinweis (84) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Set Logical Eof, Update Binary, Terminate, Write Binary.

Hinweis (85) Die Werte der Attribute fileIdentifier und shortFileIdentifier sind in [ISO7816-15] [ISO7816-4] festgelegt.

5.7.1.3 MF / DF.CIA.QES / EF.AOD (Authentication Object Directory)

Card-G2-A 2121-02 ~~Card-G2-A-2121-01~~ - K_Initialisierung: Initialisierte Attribute von MF / DF.CIA.QES / EF.AOD (Authentication Object Directory) MF / DF.CIA.QES / EF.AOD MUSS die in Tab_HBA_ObjSys_061 dargestellten Werte besitzen.

Tabelle 78: Tab_HBA_ObjSys_061 Initialisierte Attribute von MF / DF.CIA.QES / EF.AOD (Authentication Object Directory)

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	'50 34'	
shortFileIdentifier	'14' = 20	
numberOfOctet	'00 7C' Oktett = 124 Oktett	
positionLogicalEndOfFile	'00 7C' Oktett = 124 Oktett <u>numberOfOctet</u>	
flagTransactionMode	False	
flagChecksum	True	
lifeCycleStatus	Operational state (activated)	
shareable	True	

body	30 3F 30 0C 0C 07 50 49 4E 2E 51 45 53 04 01 13 30 06 04 01 03 80 01 01 A1 27 30 25 03 03 04 4C 10 0A 01 04 02 01 06 02 01 08 02 01 08 80 01 81 04 01 FF 30 0C A1 0A 4F 06 D2 76 00 00 66 01 04 00 30 39 30 09 0C 07 50 55 4B 2E 51 45 53 30 06 04 01 13 80 01 01 A1 24 30 22 03 03 02 7E 04 0A 01 04 02 01 08 02 01 08 80 01 81 04 01 FF 30 0C A1 0A 4F 06 D2 76 00 00 66 01 04 00	
------	--	--

[siehe unterhalb
dieser Tabelle](#)

Zugriffsregeln für die Kontaktschnittstelle

Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet

Zugriffsart	Zugriffsbedingung	Bemerkung
Read Binary	ALWAYS	
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	

Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
Read Binary	AUT_PACE	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

1996 [\leftarrow]30 3f
1997 | 30 0c
1998 | | 0c 07 50494e2e514553
1999 | | 04 01 13
2000 | 30 06
2001 | | 04 01 03
2002 | | 80 01 01
2003 | a1 27
2004 | | 30 25
2005 | | | 03 03 044c10
2006 | | | 0a 01 04
2007 | | | 02 01 06
2008 | | | 02 01 08
2009 | | | 02 01 08
2010 | | | 80 01 81
2011 | | | 04 01 ff
2012 | | | 30 0c
2013 | | | | a1 0a
2014 | | | | 4f 06 d27600006601
2015 | | | | 04 00
2016 30 39
2017 | 30 09
2018 | | 0c 07 50554b2e514553
2019 | 30 06
2020 | | 04 01 13
2021 | | 80 01 01
2022 | a1 24
2023 | | 30 22
2024 | | | 03 03 027e04
2025 | | | 0a 01 04
2026 | | | 02 01 08
2027 | | | 02 01 08
2028 | | | 80 01 81
2029 | | | 04 01 ff
2030 | | | 30 0c
2031 | | | | a1 0a

2032 | | | | | 4f 06 d27600006601
2033 | | | | | 04 00[<=]

2034 Hinweis (86) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF
2035 arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Set
2036 Logical Eof, Update Binary, Terminate, Write Binary.

2037

2038 5.7.1.4 MF / DF.CIA.QES / EF.PrKD (Private Key Directory)

2039 ~~Card-G2-A_2122-02~~Card-G2-A_2122-01 - K_Initialisierung: Initialisierte 2040 Attribute von MF / DF.CIA.QES / EF.PrKD (Private Key Directory)

2041 MF / DF.CIA.QES / EF.PrKD MUSS die in Tab_HBA_ObjSys_062 dargestellten Werte
2042 besitzen.

2043 Der initialisierte Wert des ASN.1 Elements *userConsent* (Oktett 26markiert mit 'xx' des
2044 ~~Attributs body, Zählweise beginnend mit 1~~Attributsbody) MUSS den Wert des SSEC für
2045 SE#1 aus MF / DF.QES / PIN.QES enthalten.

2046 **Tabelle 79: Tab_HBA_ObjSys_062 Initialisierte Attribute von MF / DF.CIA.QES / EF.PrKD**
2047 **(Private Key Directory)**

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
<i>fileIdentifier</i>	'50 35'	
<i>shortFileIdentifier</i>	'15' = 21	
<i>numberOfOctet</i>	'00 B2' Oktett = 178 Oktett, falls SSEC aus [1, 127] '00 B3' Oktett = 179 Oktett, falls SSEC aus [128, 250]	
<i>positionLogicalEndOfFile</i>	'00 B2' Oktett = 178 Oktett numberOfOctet	
<i>flagTransactionMode</i>	False	
<i>flagChecksum</i>	True	
<i>lifeCycleStatus</i>	Operational state (activated)	
<i>shareable</i>	True	
<i>body</i>	<pre> 30 59 30 2C 0C 0A 50 72 4B 2E 48 50 2E 51 45 53 03 02 07 80 04 01 03 02 01 'xx' 30 14 30 12 03 02 02 24 A1 0C 04 01 03 30 07 03 02 05 20 02 01 01 30 13 </pre>	

	04 01 84	
	03 02 05 20	
	03 02 03 B8	
	02 01 84	
	A1 03	
	02 01 01	
	A1 14	
	30 12	
	30 0C	
	A1 0A	
	4F 06 D2 76 00 00 66 01	
	04 00	
	02 02 08 00	
	A0 55	
	30 2C	
	0C 0A 50 72 4B 2E 48 50 2E 51 45	
	53	
	03 02 07 80	
	04 01 03	
	02 01 01	
	30 14	
	30 12	
	03 02 02 24	
	A1 0C	
	04 01 03	
	30 07	
	03 02 05 20	
	02 01 01	
	30 13	
	04 01 86	
	03 02 05 20	
	03 02 03 B8	
	02 01 86	
	A1 03	
	02 01 02	
	A1 10	
	30 0E	
	30 0C	
	A1 0A	
	4F 06 D2 76 00 00 66 01	
	04 00	siehe unterhalb
	dieser Tabelle	

Zugriffsregeln für die Kontaktschnittstelle

Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet

Zugriffsart	Zugriffsbedingung	Bemerkung
Read Binary	ALWAYS	
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	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
Read Binary	AUT_PACE	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

[<=] Fallunterscheidung:

a. SSEC aus [1, 127]: xx='af', yy='48' und userConsent='02 01 zz' mit 'zz' als hexadezimaler Codierung für Integer aus [1, 127] = ['01', '7f'].

b. SSEC aus [128, 250]: xx='b0', yy='49' und userConsent='02 02 zzzz' mit 'zzzz' als hexadezimaler Codierung für Integer aus [127, 250] = ['0080', '00fa'].

```

30 81xx
| 30 yy
| | 0c 0a 50724b2e48502e514553
| | 03 02 0780
| | 04 01 03
| | userConsent
| | 14 30
1203020224a10c040103300703020520020101301304018403020520030203b8020184a103020101a1143012300ca1
0a
| 4f 06 d27600006601
| 04 00
| 02 02 0800
| a0 55
| | 30 2c
| | | 0c 0a 50724b2e48502e514553
| | | 03 02 0780
| | | 04 01 03
| | | 02 01 01
| | | 30 14
| | | | 30 12
| | | | 03 02 0224
| | | | a1 0c
| | | | 04 01 03
| | | | 30 07
| | | | 03 02 0520
| | | | 02 01 01
| | 30 13
| | | 04 01 86
| | | 03 02 0520
| | | 03 02 03b8
| | | 02 01 86
| | | a1 03
| | | | 02 01 02
| | a1 10
| | | 30 0e
| | | 30 0c
| | | | a1 0a
| | | | 4f 06 d27600006601
| | | | 04 00[<=]
```

2093 Hinweis (87) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF
2094 arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Set
2095 Logical Eof, Update Binary, Terminate, Write Binary.

2096 5.7.1.5 MF / DF.CIA.QES / EF.CD (Certificate Directory)

2097 ~~Card-G2-A 2123-02~~~~Card-G2-A 2123-01~~ - K_Initialisierung: Initialisierte
2098 Attribute von MF / DF.CIA.QES / EF.CD(Certificate Directory)

2099 MF / DF.CIA.QES / EF.CD MUSS die in Tab_HBA_ObjSys_063 dargestellten Werte
2100 besitzen.

2101 **Tabelle 80: Tab_HBA_ObjSys_063 Initialisierte Attribute von MF / DF.CIA.QES / EF.CD**
2102 **(Certificate Directory)**

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	'50 38'	
shortFileIdentifier	'16' = 22	
numberOfOctet	'4E' Oktett = 78 Oktett	
positionLogicalEndOfFile	'4E' Oktett = 78 Oktett <u>numberOfOctet</u>	
flagTransactionMode	False	
flagChecksum	True	
lifeCycleStatus	Operational state (activated)	
shareable	True	
body	30 25 30 0A 0C 08 43 2E 48 50 2E 51 45 53 30 03 04 01 84 A1 12 30 10 30 0E A1 0C 4F 06 D2 76 00 00 66 01 04 02 C0 00 30 25 30 0A 0C 08 43 2E 48 50 2E 51 45 53 30 03 04 01 86	

	A1 12 30 10 30 0E A1 0C 4F 06 D2 76 00 00 66 01 04 02 C0 06	
	siehe unterhalb dieser Tabelle	

Zugriffsregeln für die Kontaktschnittstelle

Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet

Zugriffsart	Zugriffsbedingung	Bemerkung
Read Binary	ALWAYS	
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	

Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)

Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos

Zugriffsart	Zugriffsbedingung	Bemerkung
Read Binary	AUT_PACE	
andere	NEVER	

Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos

Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

Zugriffsregel für logischen LCS „Termination state“ kontaktlos

Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

[<=] 30 25

| 30 0a

| | 0c 08 432e48502e514553

| 30 03

| | 04 01 84

| a1 12

| | 30 10

```

2111 | | | 30 0e
2112 | | | | a1 0c
2113 | | | | | 4f 06 d27600006601
2114 | | | | | 04 02 c000
2115 30 25
2116 | 30 0a
2117 | | 0c 08 432e48502e514553
2118 | 30 03
2119 | | 04 01 86
2120 | a1 12
2121 | | 30 10
2122 | | | 30 0e
2123 | | | | a1 0c
2124 | | | | | 4f 06 d27600006601
2125 | | | | | 04 02 c006[<=]

```

2126 *Hinweis (88) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF*
2127 *arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Set*
2128 *Logical Eof, Update Binary, Terminate, Write Binary.*

2129 5.7.2 MF / DF.CIA.ESIGN (Cryptographic Information Applications)

2130 **Card-G2-A_2118-01 - K_Initialisierung: Initialisierte Attribute von MF /**
2131 **DF.CIA.ESIGN**

2132 DF.CIA.ESIGN MUSS die in Tab_HBA_ObjSys_058 dargestellten Werte besitzen.

2133

2134 **Tabelle 81: Tab_HBA_ObjSys_058 Initialisierte Attribute von MF / DF.CIA.ESIGN**

Attribute	Wert	Bemerkung
Objektyp	Ordner	
<i>applicationIdentifier</i>	'E828BD080F A000000167455349474E'	siehe Hinweis 90:
<i>fileIdentifier</i>	-	siehe Hinweis 91:
<i>lifeCycleStatus</i>	„Operational state (activated)“	
<i>shareable</i>	True	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
GET RANDOM	ALWAYS	
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	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
GET RANDOM	AUT_PACE	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

- 2135
2136 [**<=**]
- 2137 *Hinweis (89) Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt arbeiten,*
2138 *sind:*
2139 *Activate, Deactivate, Delete, Fingerprint, Get Random, List Public Key, Load Application,*
2140 *Select, Terminate DF.*
- 2141 *Hinweis (90) Der Wert des Attributes applicationIdentifier enthält eine RID gemäß*
2142 *[ISO7816-15] sowie als PIX den applicationIdentifier von [ISO7816-4].*
- 2143 *Hinweis (91) herstellerspezifisch; Falls unterstützt, dann außerhalb des Intervalls ['1000',*
2144 *'FEFF']; siehe [gemSpec_COS# 8.1.1]*
- 2145 *Hinweis (92) Da sich weder dieser Ordner noch darüberliegende Ebenen deaktivieren*
2146 *lassen, sind diese Zustände für Objekte im Kapitel 5.7 im Allgemeinen irrelevant.*

2147 **5.7.2.1 MF / DF.CIA.ESIGN / EF.CIA.CIAInfo**

2148 **Card-G2-A 3320-02~~Card-G2-A 3320-01~~ - K_Initialisierung: Initialisierte**

2149 **Attribute von MF / DF.CIA.ESIGN / EF.CIA.CIAInfo**

2150 MF / DF.CIA.ESIGN / EF.CIA.CIAInfo MUSS die in Tab_HBA_ObjSys_145 dargestellten
2151 Werte besitzen.

2152 **Tabelle 82: Tab_HBA_ObjSys_145 Initialisierte Attribute von MF / DF.CIA.ESIGN /**
2153 **EF.CIA.CIAInfo (Cryptographic Information Application Info)**

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	'50 32'	siehe Hinweis (94÷)
shortFileIdentifier	'12' = 18	siehe Hinweis (94÷)

<i>numberOfOctet</i>	'01 15' Oktett = 277 Oktett	
<i>positionLogicalEndOfFile</i>	<i>numberOfOctet</i>	
<i>flagTransactionMode</i>	False	
<i>flagChecksum</i>	True	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
<i>shareable</i>	True	
<i>body</i>	<pre> 30 82 01 11 02 01 01 80 11 45 53 49 47 4E 20 41 70 70 6C 69 63 61 74 69 6F 6E 03 02 05 60 A2 81 F4 30 49 02 01 01 02 01 43 30 2F A0 0F 30 0D 06 09 60 86 48 01 65 03 04 02 01 05 00 A1 1C 30 1A 06 09 2A 86 48 86 F7 0D 01 01 08 30 0D 06 09 60 86 48 01 65 03 04 02 01 05 00 03 02 06 40 06 09 2A 86 48 86 F7 0D 01 01 0A 02 01 05 30 1A 02 01 02 02 01 01 05 00 03 02 06 40 06 09 2A 86 48 86 F7 0D 01 01 01 02 01 02 30 4C 02 01 05 02 04 80 00 00 02 30 2F A0 0F 30 0D 06 09 60 86 48 01 65 03 04 02 01 05 00 A1 1C 30 1A </pre>	

	06 09 2A 86 48 86 F7	
	0D 01 01 08	
	30 0D	
	06 09 60 86 48 01 65	
	03 04 02 01	
	05 00	
	03 02 02 04	
	06 09 2A 86 48 86 F7 0D 01 01 07	
	02 01 85	
	30 1C	
	02 01 06	
	02 04 80 00 00 05	
	05 00	
	03 02 06 40	
	06 08 2A 86 48 CE 3D 04 03 02	
	02 01 00	
	30 1F	
	02 01 07	
	02 04 80 00 00 06	
	05 00	
	03 02 02 04	
	06 0B 04 00 7F 00 07 01 01	
	05 01 02 04	
	02 01 0B	siehe unterhalb dieser
	Tabelle	

Zugriffsregeln für die Kontaktschnittstelle

Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet

Zugriffsart	Zugriffsbedingung	Bemerkung
Read Binary	ALWAYS	
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	

Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)

Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos

Zugriffsart	Zugriffsbedingung	Bemerkung
Read Binary	<u>AUT_PACE</u>	

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

```

2154 f<=f30 820111
2155 | 02 01 01
2156 | 80 11 455349474e204170706c69636174696f6e
2157 | 03 02 0560
2158 | a2 81f4
2159 | | 30 49
2160 | | | 02 01 01
2161 | | | 02 01 43
2162 | | | 30 2f
2163 | | | | a0 0f
2164 | | | | | 30 0d
2165 | | | | | 06 09 608648016503040201
2166 | | | | | 05 00
2167 | | | | a1 1c
2168 | | | | | 30 1a
2169 | | | | | 06 09 2a864886f70d010108
2170 | | | | | 30 0d
2171 | | | | | 06 09 608648016503040201
2172 | | | | | 05 00
2173 | | | | 03 02 0640
2174 | | | | 06 09 2a864886f70d01010a
2175 | | | | 02 01 05
2176 | | | 30 1a
2177 | | | | 02 01 02
2178 | | | | 02 01 01
2179 | | | | 05 00
2180 | | | | 03 02 0640
2181 | | | | 06 09 2a864886f70d010101
2182 | | | | 02 01 02
2183 | | | 30 4c
2184 | | | | 02 01 05
2185 | | | | 02 04 80000002
2186 | | | | 30 2f
2187 | | | | | a0 0f
2188 | | | | | 30 0d
2189 | | | | | 06 09 608648016503040201
2190 | | | | | 05 00
2191 | | | | | a1 1c
2192 | | | | | 30 1a
2193 | | | | | 06 09 2a864886f70d010108
2194 | | | | | 30 0d
2195

```

2196 | | | | | | | 06 09 608648016503040201
2197 | | | | | | | 05 00
2198 | | | 03 02 0204
2199 | | | 06 09 2a864886f70d010107
2200 | | | 02 01 85
2201 | | 30 1c
2202 | | | 02 01 06
2203 | | | 02 04 80000005
2204 | | | 05 00
2205 | | | 03 02 0640
2206 | | | 06 08 2a8648ce3d040302
2207 | | | 02 01 00
2208 | | 30 1f
2209 | | | 02 01 07
2210 | | | 02 04 80000006
2211 | | | 05 00
2212 | | | 03 02 0204
2213 | | | 06 0b 04007f0007010105010204
2214 | | | 02 01 0b[<=]

2215 *Hinweis (93) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF*
2216 *arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Set*
2217 *Logical Eof, Update Binary, Terminate, Write Binary.*

2218 *Hinweis (94) Die Werte der Attribute fileIdentifier und shortFileIdentifier sind in*
2219 *[ISO7816-15] festgelegt.*

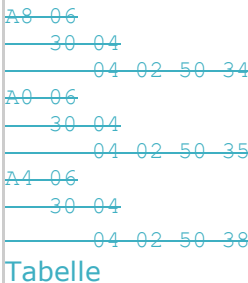
2220 5.7.2.2 MF / DF.CIA.ESIGN / EF.OD

2221 **Card-G2-A 3321-02** ~~Card-G2-A 3321-01~~ - K_Initialisierung: Initialisierte
2222 **Attribute von MF / DF.CIA.ESIGN / EF.OD (Object Directory)**

2223 MF / DF.CIA.ESIGN / EF.OD MUSS die in Tab_HBA_ObjSys_146 dargestellten Werte
2224 besitzen.

2225 **Tabelle 83: Tab_HBA_ObjSys_146 Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.OD**
2226 **(Object Directory)**

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	'50 31'	siehe Hinweis (96÷)
shortFileIdentifier	'11' = 17	siehe Hinweis (96÷)
numberOfOctet	'0018' Oktett = 224 Oktett	
positionLogicalEndOfFile	'0018' Oktett = 2 Oktett numberOfOctet	
flagTransactionMode	False	
flagChecksum	True	

lifeCycleStatus	Operational state (activated)	
shareable	True	
body	 siehe unterhalb dieser Tabelle	

Zugriffsregeln für die Kontaktschnittstelle

Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet

Zugriffsart	Zugriffsbedingung	Bemerkung
Read Binary	ALWAYS	

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	

Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)

Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos

Zugriffsart	Zugriffsbedingung	Bemerkung
Read Binary	AUT_PACE	

andere	NEVER	
--------	-------	--

Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos

Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

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

[<=]

a8 06

| 30 04

| | 04 02 5034

a0 06

| 30 04

| | 04 02 5035

a4 06

| 30 04

| | 04 02 5038 [<=]

Hinweis (95) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Set Logical Eof, Update Binary, Terminate, Write Binary.

Hinweis (96) Die Werte der Attribute fileIdentifier und shortFileIdentifier sind in [ISO7816-15] festgelegt.

5.7.2.3 MF / DF.CIA.ESIGN / EF.AOD (Authentication Object Directory)

Card-G2-A 3322-02 - K_Initialisierung: Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.AOD (Authentication Object Directory) MF / DF.CIA.ESIGN / EF.AOD MUSS die in Tab_HBA_ObjSys_147 dargestellten Werte besitzen.

Tabelle 84: Tab_HBA_ObjSys_147 Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.AOD (Authentication Object Directory)

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	'50 34'	
shortFileIdentifier	'14' = 20	
numberOfOctet	'00 58' Oktett = 88 Oktett	
positionLogicalEndOfFile	'00 58' Oktett = 88 Oktett <u>numberOfOctet</u>	
flagTransactionMode	False	

<i>flagChecksum</i>	True	
<i>lifeCycleStatus</i>	Operational state (activated)	
<i>shareable</i>	True	
<i>body</i>	<pre> 30-2D 30 0B 0C 06 50 49 4E 2E 43 48 04 01 12 30 03 04 01 02 A1 19 30 17 03 03 04 0C 10 0A 01 04 02 01 06 02 01 08 02 01 08 80 01 01 04 01 FF 30-27 30 08 0C 06 50 55 4B 2E 43 48 30 03 04 01 12 A1 16 30 14 03 03 02 3E 04 0A 01 04 02 01 08 02 01 08 80 01 01 04 01 FF </pre> <p>siehe unterhalb dieser Tabelle</p>	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
Read Binary	ALWAYS	
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	

Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
Read Binary	AUT_PACE	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

```

2251  [<=]30 2d
2252  | 30 0b
2253  | | 0c 06 50494e2e4348
2254  | | 04 01 12
2255  | 30 03
2256  | | 04 01 02
2257  | a1 19
2258  | | 30 17
2259  | | | 03 03 040c10
2260  | | | 0a 01 04
2261  | | | 02 01 06
2262  | | | 02 01 08
2263  | | | 02 01 08
2264  | | | 80 01 01
2265  | | | 04 01 ff
2266  30 27
2267  | 30 08
2268  | | 0c 06 50554b2e4348
2269  | 30 03
2270  | | 04 01 12
2271  | a1 16
2272  | | 30 14
2273  | | | 03 03 023e04
2274  | | | 0a 01 04
2275  | | | 02 01 08
2276  | | | 02 01 08
2277  | | | 80 01 01
2278  | | | 04 01 ff[<=]

```

Hinweis (97) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Set Logical Eof, Update Binary, Terminate, Write Binary.

5.7.2.4 MF / DF.CIA.ESIGN / EF.PrKD (Private Key Directory)

Card-G2-A_3323-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.PrKD (Private Key Directory)

MF / DF.CIA.ESIGN / EF.PrKD MUSS die in Tab_HBA_ObjSys_148 dargestellten Werte besitzen.

Tabelle 85: Tab_HBA_ObjSys_148 Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.PrKD (Private Key Directory)

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
<i>fileIdentifier</i>	'50 35'	
<i>shortFileIdentifier</i>	'15' = 21	
<i>numberOfOctet</i>	'02 0E' Oktett = 526 Oktett	
<i>positionLogicalEndOfFile</i>	<i>numberOfOctet</i>	
<i>flagTransactionMode</i>	False	
<i>flagChecksum</i>	True	
<i>lifeCycleStatus</i>	Operational state (activated)	
<i>shareable</i>	True	

body	<pre> 30 5B 30 27 0C 0A 50 72 4B 2E 48 50 2E 41 55 54 03 02 07 80 04 01 02 30 12 30 10 03 03 06 24 40 A1 09 04 01 02 30 04 03 02 05 20 30 16 04 01 82 03 02 05 20 03 02 03 B8 02 01 82 A1 06 02 01 01 02 01 02 A1 18 30 16 30 10 A1 0E 4F 0A A0 00 00 01 67 45 53 49 47 4E 04 00 02 02 08 00 30 57 30 26 0C 0A 50 72 4B 2E 48 50 2E 45 4E 43 03 02 07 80 04 01 02 30 11 30 0F 03 02 00 21 A1 09 04 01 02 30 04 03 02 05 20 30 13 04 01 83 03 02 06 40 03 02 03 B8 02 01 83 A1 03 02 01 05 A1 18 30 16 30 10 A1 0E 4F 0A A0 00 00 01 67 45 53 49 47 4E 04 00 02 02 08 00 30 57 30 26 0C 0A 50 72 4B 2E 48 50 2E 53 49 47 03 02 07 80 04 01 02 30 11 30 0F 03 02 02 24 </pre>	
------	---	--

	A1 09 04 01 02 30 04 03 02 05 20 30 13 04 01 84 03 02 05 20 03 02 03 B8 02 01 84 A1 03 02 01 01 A1 18 30 16 30 10 A1 0E 4F 0A A0 00 00 01 67 45 53 49 47 4E 04 00 02 02 08 00 A0 53 30 26 0C 0A 50 72 4B 2E 48 50 2E 41 55 54 03 02 07 80 04 01 02 30 11 30 0F 03 02 02 24 A1 09 04 01 02 30 04 03 02 05 20 30 13 04 01 86 03 02 05 20 03 02 03 B8 02 01 86 A1 03 02 01 06 A1 14 30 12 30 10 A1 0E 4F 0A A0 00 00 01 67 45 53 49 47 4E 04 00 A0 53 30 26 0C 0A 50 72 4B 2E 48 50 2E 45 4E 43 03 02 07 80 04 01 02 30 11 30 0F 03 02 00 21 A1 09 04 01 02 30 04 03 02 05 20 30 13 04 01 85 03 02 06 40 03 02 03 B8 02 01 85 A1 03	
--	--	--

	<pre>02 01 07 A1 14 30 12 30 10 A1 0E 4F 0A A0 00 00 01 67 45 53 49 47 4E 04 00 A0 53 30 26 0C 0A 50 72 4B 2E 48 50 2E 53 49 47 03 02 07 80 04 01 02 30 11 30 0F 03 02 02 24 A1 09 04 01 02 30 04 03 02 05 20 30 13 04 01 87 03 02 05 20 03 02 03 B8 02 01 87 A1 03 02 01 06 A1 14 30 12 30 10 A1 0E 4F 0A A0 00 00 01 67 45 53 49 47 4E 04 00</pre>	
--	--	--

Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
Read Binary	ALWAYS	
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	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
Read Binary	AUT_PACE	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung

alle	herstellerspezifisch	
------	----------------------	--

2290

2291 [\leq]

2292 Hinweis (98) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF
2293 arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Set
2294 Logical Eof, Update Binary, Terminate, Write Binary.

2295 5.7.2.5 MF / DF.CIA.ESIGN / EF.CD (Certificate Directory)

2296 Card-G2-A_3324-01 - K_Initialisierung: Initialisierte Attribute von MF /
2297 DF.CIA.ESIGN / EF.CD (Certificate Directory)

2298 MF / DF.CIA.ESIGN / EF.CD MUSS die in Tab_HBA_ObjSys_149 dargestellten Werte
2299 besitzen.

2300

2301 **Tabelle 86: Tab_HBA_ObjSys_149 Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.CD**
2302 **(Certificate Directory)**

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	
fileIdentifier	'50 38'	
shortFileIdentifier	'16' = 22	
numberOfOctet	'01 02' Oktett = 258 Oktett	
positionLogicalEndOfFile	numberOfOctett	
flagTransactionMode	False	
flagChecksum	True	
lifeCycleStatus	Operational state (activated)	
shareable	True	
body	<pre> 30 29 30 0A 0C 08 43 2E 48 50 2E 41 55 54 30 03 04 01 82 A1 16 30 14 30 12 A1 10 4F 0A A0 00 00 01 67 45 53 49 47 </pre>	

	4E	
	04 02 C5 00	
30 29		
30 0A		
	0C 08 43 2E 48 50 2E 45 4E	
43		
30 03		
	04 01 83	
A1 16		
30 14		
30 12		
A1 10		
	4F 0A A0 00 00 01	
67		
	45 53 49 47	
4E		
	04 02 C2 00	
30 29		
30 0A		
	0C 08 43 2E 48 50 2E 53 49	
47		
30 03		
	04 01 84	
A1 16		
30 14		
30 12		
A1 10		
	4F 0A A0 00 00 01	
67		
	45 53 49 47	
4E		
	04 02 C0 00	
30 29		
30 0A		
	0C 08 43 2E 48 50 2E 41 55	
54		
30 03		
	04 01 86	
A1 16		
30 14		
30 12		
A1 10		
	4F 0A A0 00 00 01	
67		
	45 53 49 47 4E	
	04 02 C5 06	
30 29		
30 0A		
	0C 08 43 2E 48 50 2E 45 4E	
43		
30 03		
	04 01 85	
A1 16		
30 14		
30 12		
A1 10		
	4F 0A A0 00 00 01	
67		
	45 53 49 47	
4E		
	04 02 C2 05	
30 29		
30 0A		

<pre> 0C 08 43 2E 48 50 2E 53 49 47 30 03 04 01 87 A1 16 30 14 30 12 A1 10 4F 0A A0 00 00 01 67 45 53 49 47 4E 04 02 C0 07 </pre>		
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
Read Binary	ALWAYS	
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	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
Read Binary	AUT_PACE	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		

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

2303
2304

[<=]

2305 *Hinweis (99) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF*
2306 *arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Set*
2307 *Logical Eof, Update Binary, Terminate, Write Binary.*

2308 5.8 Die Organisationsspezifische Authentisierungsanwendung

2309 Die organisationsspezifische Authentisierungsanwendung DF.AUTO ist eine Anwendung,
2310 deren Struktur auf einem HBA stets vorhanden ist. Es liegt im Ermessen der HBA-
2311 Herausgeberorganisation (Berufskammer), ob die Anwendung nutzbar gemacht werden
2312 kann. Die eigentliche Nutzung der Anwendung liegt im Ermessen des Karteninhabers.
2313 Falls die organisationsspezifische Authentisierungsanwendung genutzt wird, dann ist der
2314 Inhalt dieses Kapitels verbindlich vorgeschrieben.

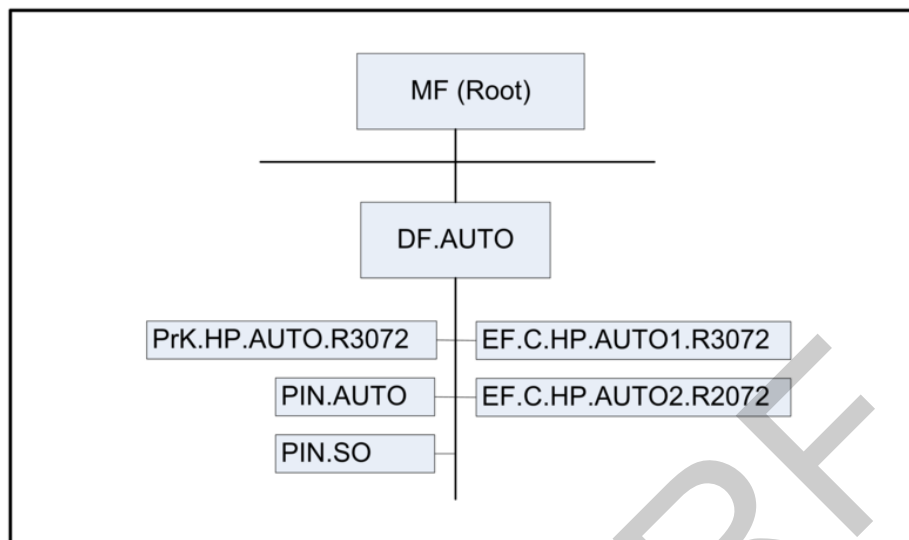
2315 5.8.1 Dateistruktur und Dateinhalt

2316 DF.AUTO wird genutzt für

- 2317 • organisationsspezifische Authentisierungsprozesse (z. B. Windows Logon mit
2318 Smart Card), welche mit der ESIGN-Anwendung aufgrund technischer
2319 Unterschiede (z. B. proprietäre Zertifikatserweiterungen) oder eines
2320 unvereinbaren Verfahrens (z. B. vorgeschriebenes PIN-Caching) nicht
2321 umgehen können.

2322 Die Abbildung Abb_HBA_ObjSys_006 zeigt die prinzipielle Struktur der AUTO-
2323 Anwendung.

2324



2325

2326

2327

Abbildung 6: Abb_HBA_ObjSys_006 Prinzipielle Struktur von DF.AUTO

2328

5.8.2 DF.AUTO (Organization-specific Authentication Application)

2329

DF.AUTO ist ein "Application Directory" gemäß [gemSpec_COS#8.3.1.1], d.h., es ist mittels Anwendungskennung selektierbar.

2330

2331

Card-G2-A_2124-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.AUTO

2332

2333

DF.AUTO MUSS die in Tab_HBA_ObjSys_064 dargestellten Werte besitzen.

2334

2335

Tabelle 87: Tab_HBA_ObjSys_064 Initialisierte Attribute von MF / DF.AUTO

Attribute	Wert	Bemerkung
Objekttyp	Ordner	
<i>applicationIdentifier</i>	'D27600014603'	siehe Hinweis 101:
<i>fileIdentifier</i>	-	siehe Hinweis 102:
<i>lifeCycleStatus</i>	„Operational state (activated)“	
<i>shareable</i>	True	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
GET RANDOM	ALWAYS	
LOAD APPLICATION	AUT_CMS	siehe Hinweis 104:

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	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
GET RANDOM	AUT_PACE	
LOAD APPLICATION	AUT_CMS	siehe Hinweis 104:
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

- 2336
2337 **[<=]**
- 2338 *Hinweis (100) Kommandos, die gemäß [gemSpec_COS] mit einem Ordnerobjekt*
2339 *arbeiten, sind:*
2340 *Activate, Deactivate, Delete, Fingerprint, Get Random, List Public Key, Load Application,*
2341 *Select, Terminate DF.*
- 2342 *Hinweis (101) Der Wert des Attributes applicationIdentifier ist in [ISO7816-4].*
- 2343 *Hinweis (102) herstellerepezifisch; falls unterstützt, dann außerhalb des Intervalls*
2344 *['1000', 'FEFF']; siehe [gemSpec_COS#8.1.1]*
- 2345 *Hinweis (103) Da sich weder dieser Ordner noch darüberliegende Ebenen deaktivieren*
2346 *lassen, sind diese Zustände für Objekte im Kapitel 5.8 im Allgemeinen irrelevant.*
- 2347 *Hinweis (104) Das Kommando ist nur vom Inhaber des CMS-Schlüssels ausführbar, siehe*
2348 *Kapitel 5.9.*

5.8.2.1 MF / DF.AUTO / PrK.HP.AUTO.R3072

PrK.HP.AUTO.R3072 ist der private Schlüssel für die Kryptographie mit RSA für Client-/Server-Authentisierung.

Card-G2-A_2125-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.AUTO / PrK.HP.AUTO.R3072

PrK.HP.AUTO.R3072 MUSS die in Tab_HBA_ObjSys_065 dargestellten Werte besitzen.

Tabelle 88: Tab_HBA_ObjSys_065 Initialisierte Attribute von MF / DF:AUTO / PrK.HP.AUTO.R3072

Attribute	Wert	Bemerkung
Objektyp	privates Schlüsselobjekt, RSA 3072	
keyIdentifizier	'02' = 2	
privateKey	herstellerspezifisch „unbefüllt“, Speicherplatz hinreichend für einen Schlüssel mit Modulslänge 3072 Bit	wird personalisiert
keyAvailable	WildCard	
listAlgorithmIdentifizier	alle Werte aus der Menge, siehe [gemSpec_COS] {rsaClientAuthentication, signPKCS1_V1_5, signPSS}	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
Generate Asymmetric Key Pair P1='81'	ALWAYS	
Internal Authenticate PSO Compute Digital Signature	PWD(PIN.AUTO)	
Delete	PWD(PIN.SO)	
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	

Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
Generate Asymmetric Key Pair P1='81'	AUT_PACE	
Internal Authenticate PSO Compute Digital Signature	AUT_PACE AND PWD(PIN.AUTO)	
Delete	AUT_PACE AND PWD(PIN.SO)	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	NEVER	

[<=]

*Hinweis (105) 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*

Anmerkung –PrK.HP.AUTO.R3072 ist ein privates RSA-Objekt, welches gemäß Kapitel 9.6.3 in [gemSpec_COS] das Kommando Generate Asymmetric Key Pair unterstützt. Da die organisationsspezifische Zertifikatsinformation dem Personalisierer wahrscheinlich nicht bekannt ist, kann es notwendig sein, dieses Kommando während der Kartennutzung zu verwenden, um eine Generierung von Zertifikaten zu ermöglichen.

Card-G2-A_3314-01 - K_Personalisierung: Personalisierte Attribute von MF / DF.AUTO / PrK.HP.AUTO.R3072

Bei der Personalisierung von PrK.HP.AUTO.R3072 MÜSSEN die in Tab_HBA_ObjSys_138 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 89: Tab_HBA_ObjSys_138 Personalisierte Attribute von MF / DF.AUTO / PrK.HP.AUTO.R3072

Attribute	Wert	Bemerkung
privateKey	Moduluslänge 3072 Bit	wird personalisiert
keyAvailable	True	

2377
2378 [\leq]

2379 In Bezug auf die Schlüssellängen müssen dieselben Konventionen wie für die Schlüssel
2380 der qualifizierten elektronischen Signatur berücksichtigt werden, siehe [ALGCAT] und
2381 [TR-03116-1].

2382 **5.8.2.2 MF / DF.AUTO / PIN.AUTO**

2383 PIN.AUTO ist eine DF-spezifische PIN, die ausschließlich dem Schutz des privaten
2384 Authentisierungsschlüssels für den organisationsspezifischen
2385 Authentisierungsmechanismus des Heilberufers (PrK.HP.AUTO.R3072) dient.

2386 Die Nutzung eines 8-stelligen Rücksetzcodes (Personal Unblocking Key, PUK) wird durch
2387 einen Nutzungszähler beschränkt, dessen Anfangswert auf 10 gesetzt ist. Der
2388 Sicherheitsstatus von PIN.AUTO kann unbegrenzt verwendet werden, d. h. der Default-
2389 Wert von SSEC beträgt unendlich.

2390 Die nachfolgende Tabelle Tab_HBA_ObjSys_068 zeigt die PIN-Referenz, wie sie in den
2391 Kommandos Verify, Change Reference Data und Reset Retry Counter verwendet wird,
2392 und weitere PIN-Eigenschaften.

2393

2394 **Card-G2-A_2128 - K_Initialisierung: Initialisierte Attribute von MF / DF.AUTO /** 2395 **PIN.AUTO**

2396 PIN.AUTO MUSS die in Tab_HBA_ObjSys_068 dargestellten Werte besitzen.

2397

2398 **Tabelle 90: Tab_HBA_ObjSys_068 Initialisierte Attribute von MF / DF.AUTO / PIN.AUTO**

Attribute	Wert	Bemerkung
Objektyp	Passwortobjekt	
<i>pwdIdentifier</i>	'01' = 1	
<i>secret</i>	undefiniert	wird personalisiert
<i>minimumLength</i>	5	
<i>maximumLength</i>	8	
<i>startRetryCounter</i>	3	
<i>retryCounter</i>	3	
<i>transportStatus</i>	ein Wert aus der Menge {Leer-PIN, Transport-PIN}	
<i>flagEnabled</i>	True	

<i>startSsec</i>	unendlich	
<i>PUK</i>	undefiniert	wird personalisiert
<i>pukUsage</i>	10	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
CHANGE RD, P1=0	ALWAYS	Hinweis 101:
CHANGE RD, P1=1	ALWAYS	Hinweis 102:
	herstellerspezifisch	siehe Card-G2-A_3270
GET PIN STATUS	ALWAYS	
RESET RC., P1=1	ALWAYS	
VERIFY	ALWAYS	
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	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
CHANGE RD, P1=0	AUT_PACE	Hinweis 107:

CHANGE RD, P1=1	AUT_PACE	Hinweis 108:
	Herstellerspezifisch unter Verwendung von AUT_PACE	siehe Card-G2- A_3270
GET PIN STATUS	AUT_PACE	
RESET RC., P1=1	AUT_PACE	
VERIFY	AUT_PACE	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

[<=]

Hinweis (106) 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.

Hinweis (107) Diese Tabellenzeile gilt für den Fall transportStatus ungleich Leer-PIN.

Hinweis (108) Diese Tabellenzeile gilt für den Fall transportStatus gleich Leer-PIN

Card-G2-A_3270 - K_Initialisierung: CHANGE REFERENCE DATA bei Nutzung der Leer-PIN für PIN.AUTO

Wenn für PIN.AUTO als Transportschutz Leer-PIN verwendet wird, dann DARF PIN.AUTO 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 herstellerepezifisch umzusetzen.

[<=]

Card-G2-A_3315 - K_Personalisierung: Personalisierte Attribute von MF / DF.AUTO / PIN.AUTO

Wenn der Wert des Attributes *transportStatus* von PIN.AUTO Transport-PIN ist, MÜSSEN bei der Personalisierung von PIN.AUTO die in Tab_HBA_ObjSys_141 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 91: Tab_HBA_ObjSys_141 Personalisierte Attribute von MF / DF.AUTO / PIN.AUTO

Attribute	Wert	Bemerkung
<i>secret</i>	PIN-Wert gemäß [gemSpec_PINPUK_TI]	Transport-PIN
<i>secretLength</i>	4 Ziffern (<i>minimumLength</i> - 1)	Länge der Transport-PIN
<i>PUK</i>	PUK-Wert gemäß [gemSpec_PINPUK_TI]	
<i>PUKLength</i>	8 Ziffern	

[<=]

Die Initialisierung von PIN.AUTO, z. B. durch Nutzung einer Transport-PIN, unterliegt den Richtlinien der zuständigen Organisation. Falls eine Transport-PIN verwendet wird, so muss ein Verfahren aus [gemSpec_COS#8.2.5] zum Einsatz kommen.

5.8.2.3 MF / DF.AUTO / PIN.SO

PIN.SO ist eine DF-spezifische PIN, die für administrative Zwecke bezüglich DF.AUTO verwendet wird, d. h. zur Generierung des asymmetrischen Schlüsselpaars und zum Aktualisieren der organisationsspezifischen Authentisierungszertifikate. PIN.SO besteht aus 6 bis 8 Ziffern.

Die Nutzung eines 8-stelligen Rücksetzcodes (Personal Unblocking Key, PUK) wird durch einen Nutzungszähler beschränkt, dessen Anfangswert auf 10 gesetzt ist. Der Sicherheitsstatus von PIN.SO kann unbegrenzt verwendet werden, d. h. der Default-Wert von SSEC beträgt unendlich.

Die nachfolgende Tabelle Tab_HBA_ObjSys_069 zeigt die PIN-Referenz, wie sie in den Kommandos Verify, Change Reference Data und Reset Retry Counter verwendet wird, und weitere PIN-Eigenschaften.

Card-G2-A_2129 - K_Initialisierung: Initialisierte Attribute von MF / DF.AUTO / PIN.SO

PIN.SO MUSS die in Tab_HBA_ObjSys_069 dargestellten Werte besitzen.

Tabelle 92: Tab_HBA_ObjSys_069 Initialisierte Attribute von MF / DF.AUTO / PIN.SO

Attribute	Wert	Bemerkung
Objekttyp	Passwortobjekt	
<i>pwdIdentifier</i>	'03' = 3	
<i>secret</i>	undefiniert	wird personalisiert
<i>minimumLength</i>	6	

<i>maxLength</i>	8	
<i>startRetryCounter</i>	3	
<i>retryCounter</i>	3	
<i>transportStatus</i>	ein Wert aus der Menge {Leer-PIN, Transport-PIN}	
<i>flagEnabled</i>	True	
<i>startSsec</i>	unendlich	
<i>PUK</i>	undefiniert	wird personalisiert
<i>pukUsage</i>	10	
<i>lifeCycleStatus</i>	„Operational state (activated)“	
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
CHANGE RD, P1=0	ALWAYS	Hinweis 105:
CHANGE RD, P1=1	ALWAYS	Hinweis 106:
	herstellerspezifisch	siehe Card-G2-A_3271
GET PIN STATUS	ALWAYS	
RESET RC., P1=1	ALWAYS	
VERIFY	ALWAYS	
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	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
CHANGE RD, P1=0	AUT_PACE	Hinweis 111:
CHANGE RD, P1=1	AUT_PACE	Hinweis 112:
	Herstellerspezifisch unter Verwendung von AUT_PACE	siehe Card-G2- A_3271
GET PIN STATUS	AUT_PACE	
RESET RC., P1=1	AUT_PACE	
VERIFY	AUT_PACE	
andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

2446
2447

[<=]

2448 *Hinweis (110) Kommandos, die gemäß [gemSpec_COS] mit einem Passwortobjekt*
 2449 *arbeiten, sind: Activate, Change Reference Data, Deactivate, Delete, Disable Verification*
 2450 *Requirement, Enable Verification Requirement, Get Pin Status, Reset Retry Counter,*
 2451 *Verify, Terminate.*

2452 *Hinweis (111) Diese Tabellenzeile gilt für den Fall transportStatus ungleich Leer-PIN.*

2453 *Hinweis (112) Diese Tabellenzeile gilt für den Fall transportStatus gleich Leer-PIN*
 2454

Card-G2-A_3271 - K_Initialisierung: CHANGE REFERENCE DATA bei Nutzung der Leer-PIN für PIN.SO

Wenn für PIN.SO als Transportschutz Leer-PIN verwendet wird, dann DARF PIN.SO 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.
[<=]

Card-G2-A_3316 - K_Personalisierung: Personalisierte Attribute von MF / DF.AUTO / PIN.SO

Wenn der Wert des Attributes *transportStatus* von PIN.SO Transport-PIN ist, MÜSSEN bei der Personalisierung von PIN.SO die in Tab_HBA_ObjSys_142 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 93: Tab_HBA_ObjSys_142 Personalisierte Attribute von MF / DF.AUTO / PIN.SO

Attribute	Wert	Bemerkung
<i>secret</i>	PIN-Wert gemäß [gemSpec_PINPUK_TI]	Transport-PIN
<i>secretLength</i>	5 Ziffern (<i>minimumLength</i> - 1)	Länge der Transport-PIN
<i>PUK</i>	PUK-Wert gemäß [gemSpec_PINPUK_TI]	
<i>PUKLength</i>	8 Ziffern	

[<=]

Die Initialisierung von PIN.SO, z. B. durch Nutzung einer Transport-PIN, unterliegt den Richtlinien der zuständigen Organisation. Falls eine Transport-PIN verwendet wird, so muss ein Verfahren aus [gemSpec_COS#8.2.5] zum Einsatz kommen.

5.8.2.4 MF / DF.AUTO / EF.C.HP.AUTO1.R3072 und MF / DF.AUTO / EF.C.HP.AUTO2.R3072

EF.C.HP.AUTO1.R3072 und EF.C.HP.AUTO2.R3072 enthalten die organisationsspezifischen X.509-AUT-Zertifikate des Heilberufers für die Kryptographie mit RSA. Damit können dem Heilberufers zwei verschiedene Identitäten zur Verfügung stehen, die beide mit demselben privaten Schlüssel PrK.HP.AUTO.R3072 verknüpft sind.

Die Zertifikate können nach erfolgreicher Authentisierung mit PIN.SO aktualisiert werden, siehe Tab_HBA_ObjSys_070 und Tab_HBA_ObjSys_071.

Card-G2-A_2130-02Card-G2-A_2130-01 - K_Initialisierung: Initialisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO1.R3072

EF.C.HP.AUTO1.R3072 MUSS die in Tab_HBA_ObjSys_070 dargestellten Werte besitzen.

Tabelle 94: Tab_HBA_ObjSys_070 Initialisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO1.R3072

Attribute	Wert	Bemerkung
Objekttyp	transparentes Elementary File	

<i>fileIdentifier</i>	'E0 01'	
<i>shortFileIdentifier</i>	'01' = 1	
<i>numberOfOctet</i>	'0B B8' Oktett = 3000 Oktett	
<i>positionLogicalEndOfFile</i>	'0' Wildcard	siehe Card-G2-A 2673
<i>flagTransactionMode</i>	True	
<i>flagChecksum</i>	False	
<i>lifeCycleStatus</i>	Operational state (activated)	
<i>shareable</i>	True	
<i>body</i>	kein Inhalt	wird personalisiert
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
Delete	PWD(PIN.SO)	
Read Binary	ALWAYS	
Delete Erase Binary Set Logical EOF Update Binary Write Binary	PWD(PIN.SO)	
andereRead Binary	ALWAYS 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	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		

Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
Delete	AUT_PACE AND PWD(PIN.SO)	
Read Binary	AUT_PACE	
Delete Erase Binary Set Logical EOF Update Binary Write Binary	AUT_PACE AND PWD(PIN.SO)	
andereRead Binary	NEVERAUT_PACE	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

[<=]

Hinweis (114) Kommandos, die gemäß [gemSpec_COS] mit einem transparenten EF arbeiten, sind: Activate, Deactivate, Delete, Erase Binary, Read Binary, Select, Set Logical Eof, Update Binary, Terminate, Write Binary.

Card-G2-A 3317-02 Card-G2-A-3317-01 - K_Personalisierung: Personalisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO1.R3072

Bei der Personalisierung von EF.C.HP.AUTO1.R3072 MÜSSEN die in Tab_HBA_ObjSys_143 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 95: Tab_HBA_ObjSys_143 Personalisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO1.R3072

Attribute	Wert	Bemerkung
positionLogicalEndOfFile	Zahl der tatsächlich belegten Oktette <u>Wildcard</u>	wird personalisiert siehe Card-G2-A 2673
body	C.HP.AUTO1.R3072 gemäß [gemSpec_PKI] passend zu dem privaten Schlüssel in PrK.HP.AUTO.R3072	wird personalisiert

~~[<=]~~ [<=]

5.8.2.5 MF / DF.AUTO / EF.C.HP.AUTO2.R3072

Card-G2-A 2131-02 - K_Initialisierung: Initialisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO2.R3072

EF.C.HP.AUTO2.R3072 MUSS die in Tab_HBA_ObjSys_071 dargestellten Werte besitzen.

Tabelle 96: Tab_HBA_ObjSys_071 Initialisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO2.R3072

Attribute	Wert	Bemerkung
Objektyp	transparentes Elementary File	
fileIdentifier	'E0 02'	
shortFileIdentifier	'02' = 2	
numberOfOctet	'0B B8' Oktett = 3000 Oktett	
positionLogicalEndOfFile	'0' Wildcard	siehe Card-G2-A 2673
flagTransactionMode	True	
flagChecksum	False	
lifeCycleStatus	Operational state (activated)	
shareable	True	
body	kein Inhalt	wird personalisiert
Zugriffsregeln für die Kontaktschnittstelle		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktbehaftet		
Zugriffsart	Zugriffsbedingung	Bemerkung
Delete	PWD(PIN.SO)	
Read Binary	ALWAYS	
Delete Erase Binary Set Logical EOF Update Binary Write Binary	PWD(PIN.SO)	
andere Read Binary	ALWAYS 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	
Zugriffsregeln für die kontaktlose Schnittstelle (falls vorhanden)		
Zugriffsregel für logischen LCS „Operational state (activated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
Delete	AUT_PACE AND PWD(PIN.SO)	
Read Binary	AUT_PACE	
Delete Erase Binary Set Logical EOF Update Binary Write Binary	AUT_PACE AND PWD(PIN.SO)	
andereRead Binary	AUT_PACE NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	
Zugriffsregel für logischen LCS „Termination state“ kontaktlos		
Zugriffsart	Zugriffsbedingung	Bemerkung
alle	herstellerspezifisch	

[<=][<=]

Card-G2-A 3318-02 - K_Personalisierung: Personalisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO2.R3072

Bei der Personalisierung von EF.C.HP.AUTO2.R3072 MÜSSEN die in Tab_HBA_ObjSys_144 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 97: Tab_HBA_ObjSys_144 Personalisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO2.R3072

Attribute	Wert	Bemerkung
positionLogicalEndOfFile	Zahl der tatsächlich belegten Oktette Wildcard	wird personalisiert siehe Card-G2-A 2673

body	C.HP.AUTO2.R3072 gemäß [gemSpec_PKI] wird personalisiert passend zu dem privaten Schlüssel in PrK.HP.AUTO.R3072	
------	---	--

2517 [\leq]

2518 5-8-2-55.8.2.6 Sicherheitsumgebungen

2519 In DF.AUTO wird ausschließlich das voreingestellte SE#1 verwendet.

2520 5-8-2-65.8.2.7 Vorgaben für die Nutzung von DF.AUTO

2521 Falls die HBA-Herausgeberorganisation (Berufskammer) die Nutzung der Anwendung
2522 ermöglichen will, dann gilt bezüglich der zu personalisierenden Daten:

2523 Card-G2-A_2675-01 - K_Initialisierung: Initialisierte: Wert von 2524 PrK.HP.AUTO.R3072

2525 PrK.HP.AUTO.R3072 MUSS auf einen kartenindividuellen Wert gesetzt werden.

2526 [\leq]

2527 Card-G2-A_2676-01 Card-G2-A_2676 - K_Personalisierung: Wert von PIN.AUTO

2528 FallsWenn das Attribut „Attribute PIN.AUTO ->transportStatus“ von PIN.AUTO auf einen
2529 Wert aus der Menge {regularPassword, Transport-PIN} gesetzt ist, hat, dann MUSS die
2530 Personalisierung den Wert des Attributes PIN.AUTO ->secret auf einen
2531 kartenindividuellen Wert setzen.gesetzt werden.

2532 [\leq]

2533 Card-G2-A_2677 - K_Personalisierung: Wert von PUK für PIN.AUTO

2534 PUK für PIN.AUTO MUSS auf einen kartenindividuellen Wert gesetzt werden.

2535 [\leq]

2536 Card-G2-A_2678-01 Card-G2-A_2678 - K_Personalisierung: Wert von PIN.SO

2537 FallsWenn das Attribut „Attribute PIN.SO ->transportStatus“ von PIN.SO auf einen Wert
2538 aus der Menge {regularPassword, Transport-PIN} gesetzt ist, hat, dann MUSS die
2539 Personalisierung den Wert des Attributes PIN.SO ->secret auf einen kartenindividuellen
2540 Wert setzen.gesetzt werden.

2541 [\leq]

2542 Card-G2-A_2679 - K_Personalisierung: Wert von PUK für PIN.SO

2543 PUK für PIN.SO MUSS auf einen kartenindividuellen Wert gesetzt werden.

2544 [\leq]

2545 Card-G2-A_2680-02 Card-G2-A_2680-01 - K_Personalisierung: Inhalt von 2546 EF.C.HP.AUTO1.R3072

2547 Falls die Personalisierung in EF.C.HP.AUTO1.R3072 KANN einen beliebigen Wert
2548 enthalten. Falls hier kein passendes

2549 1. Informationen (X.509 -Zertifikat eingetragen ist, so liegt es im Ermessen des
2550 Karteninhabers, ein passendes X.509-Zertifikat einzutragen.

2551 [\leq] einträgt, dann MUSS die Personalisierung den Wert von
2552 positionLogicalEndOfFile gemäß Card-G2-A_2673 setzen.

2553 2. keine Informationen einträgt, so liegt es im Ermessen des Karteninhabers, ein
2554 passendes X.509 Zertifikat einzutragen.

2555 [\leq]

Card-G2-A_2681-02 - K_Personalisierung: Inhalt von EF.C.HP.AUTO2.R3072

Falls die Personalisierung in EF.C.HP.AUTO2.R3072 ~~KANN~~ einen beliebigen Wert enthalten. Falls hier kein passendes

1. Informationen (X.509-Zertifikat ~~eingetragen ist~~) einträgt, dann MUSS die Personalisierung den Wert von *positionLogicalEndOfFile* gemäß Card-G2-A_2673 setzen.

1.2. keine Informationen einträgt, so liegt es im Ermessen des Karteninhabers, ein passendes X.509-Zertifikat einzutragen.

[<=]

Card-G2-A_2682 - K_Personalisierung: Unterbindung der Nutzung von DF.AUTO – PIN.AUTO

Falls die HBA-Herausgeberorganisation (Berufskammer) die Nutzung der Anwendung DF.AUTO unterbinden will, dann DARF sich der Sicherheitszustand von PIN.AUTO NICHT setzen lassen.

[<=]

Card-G2-A_2856 - K_Personalisierung: Unterbindung der Nutzung von DF.AUTO – PIN.SO

Falls die HBA-Herausgeberorganisation (Berufskammer) die Nutzung der Anwendung DF.AUTO unterbinden will, dann DARF sich der Sicherheitszustand von PIN.SO NICHT setzen lassen.

[<=]

Hinweis (115) Um das Setzen eines Sicherheitszustandes zu unterbinden wird es als hinreichend angesehen, wenn die Attribute "Secret" und "PUK" eines Passwortobjektes auf zufällige acht- bis zwölfstellige Werte gesetzt werden.

5.9 Laden einer neuen Anwendung oder Anlegen eines EFs nach Ausgabe des HBA

Es wird angenommen, dass das Laden neuer Anwendungen oder das Erstellen neuer EFs auf MF-Ebene (einschließlich Aktualisieren der Dateien und EF.Version2) nach der Ausgabe des HBA von einem Card Application Management System (CMS) durchgeführt wird. Dies ist ein optionaler Prozess.

Ebenso ist das CMS optional. Die Inhalte in [gemSpec_COS#14] sind allerdings normativ, wenn das Laden neuer Anwendungen oder das Erstellen neuer EFs nach Ausgabe des HBA durchgeführt werden sollen.

2592

6 Anhang A – Verzeichnisse

2593

6.1 Abkürzungen

Kürzel	Erläuterung
AID	Application Identifier (Anwendungskennung)
AOD	Authentication Object Directory
APDU	Application Protocol Data Unit
ASN.1	Abstract Syntax Notation One
ASCII	American Standard Code for Information Interchange
AT	Authentication Template
ATR	Answer-to-Reset
AUT	Authentisierung
AUTD	CV-basierte Geräteauthentisierung
AUTR	CV-basierte Rollenauthentisierung
AUTO	Organisationsspezifische Authentisierung
BA	Berufsausweis
BCD	Binary Coded Decimal
BER	Basic Encoding Rules
BNA	Bundesnetzagentur
C	Zertifikat
C2C	Card to Card
CA	Certification Authority (Zertifizierungsdiensteanbieter)
CAR	Certification Authority Reference

CC	Cryptographic Checksum (kryptographische Prüfsumme)
CD	Certificate Directory
CER	Canonical Encoding Rules
CG	Cryptogram
CH	Cardholder (Karteninhaber)
CHAT	Certificate Holder Authorisation Template Liste von Rechten, die ein Zertifikatsinhaber besitzt
CHR	Certificate Holder Reference
CIA	Cryptographic Information Application
CIO	Cryptographic Information Objects
CLA	Class-Byte einer Kommando-APDU
CMS	Card Management System
COS	Card Operating System (Chipkartenbetriebssystem)
CPI	Certificate Profile Identifier
CRL	Certificate Revocation List (Zertifikatssperrliste)
CS	CertSign (CertificateSigning)
CTA	Card Terminal Application (Kartenterminalanwendung)
CUP	Certificate Update
CV	Card Verifiable
CVC	Card Verifiable Certificate
D,DIR	Directory
DE	Datenelement
DER	Distinguished Encoding Rules
DES	Daten Encryption Standard

DF	Dedicated File
DI	Baud rate adjustment factor
DM	Display Message
DO	Datenobjekt
DS	Digital Signature
DSI	Digital Signature Input
DTBS	Data to be signed
EF	Elementary File
eGK	elektronische Gesundheitskarte
EHIC	European Health Insurance Card
eIDAS	Verordnung über elektronische Identifizierung und Vertrauensdienste
ELC	Elliptic Curve Cryptography, Kryptographie mittels elliptischer Kurven
ENC	Encryption
ES	Electronic Signature
FCI	File Control Information
FCP	File Control Parameter
FI	Clock rate conversion factor
FID	File Identifier
GDO	Global Data Object
GKV	Gesetzliche Krankenversicherung
GP	Global Plattform
HB	Historical Bytes
HCI	Health Care Institution (Institution des Gesundheitswesens)
HP	Health Professional (Heilberufler)

HPA	Health Professional Application
HPC	Health Professional Card (Heilberufsausweis)
HPD	Health Professional related Data
ICC	Integrated Circuit Card (Chipkarte)
ICCSN	ICC Serial Number (Chip-Seriennummer)
ICM	IC Manufacturer (Kartenhersteller)
ID	Identifizier
IFSC	Information Field Size Card
IIN	Issuer Identification Number
INS	Instruction-Byte einer Kommando-APDU
KM	Komfortmerkmal
KT	Kartenterminal
LCS	Life Cycle Status
LSB	Least Significant Byte(s)
MAC	Message Authentication Code
MF	Master File
MII	Major Industry Identifier
MSE	Manage Security Environment
OCSP	Online Certificate Status Protocol
OD	Object Directory
OID	Object Identifier
OSIG	Organisationssignatur
PIN	Personal Identification Number
PIX	Proprietary Application Provider Extension

PK, PuK	Public Key
PKCS	Public Key Cryptography Standard (hier PKCS#1)
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure for X.509 Certificates (IETF)
PrK	Private Key
PSO	Perform Security Operation
PUK	Personal Unblocking Key (Resetting Code)
PV	Plain Value
P1	Parameter P1 einer Kommando-APDU
P2	Parameter P2 einer Kommando-APDU
QES	Qualifizierte Elektronische Signatur
RA	Registration Authority (Registrierungsinstanz)
RAM	Random Access Memory
RC	Retry Counter (Fehlbedienungs-zähler)
RCA	Root CA
RD	Referenzdaten
RF	Radio Frequency
RFC	Request für Comment
RFID	Radio Frequency Identification
RFU	Reserved for future use
RID	Registered Application Provider Identifier
RND	Random Number (Zufallszahl)
ROM	Read Only Memory
RPE	Remote PIN-Empfänger

RPS	Remote PIN-Sender
RSA	Algorithmus von Rivest, Shamir, Adleman
SAK	Signaturanwendungskomponente
SE	Security Environment (Sicherheitsumgebung)
SFID	Short EF Identifier
SIG	Signatur
SK	Secret Key
SM	Secure Messaging
SMA	Security Module Application
SMC	Security Module Card
SMD	Security Module Data
SMKT	Sicherheitsmodul Kartenterminal
SN	Seriennummer
SO	Security Officer (Administrator)
SSCD	Secure Signature Creation Device (Sichere Signaturerstellungseinheit)
SSEC	Security Status Evaluation Counter
SSEE	Sichere Signaturerstellungseinheit
SSL	Security Sockets Layer
SUK	Stapel- und Komfortsignatur
TLV	Tag Length Value
TC	Trusted Channel
TLS	Transport Layer Security
ZDA	Zertifizierungsdiensteanbieter

6.2 Glossar

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

6.3 Abbildungsverzeichnis

Abbildung 1: Abb_HBA_ObjSys_001 Allgemeine Dateistruktur eines HBA	25
Abbildung 2: Abb_HBA_ObjSys_002 Dateistruktur von DF.HPA	68
Abbildung 3: Abb_HBA_ObjSys_003 Prinzipielle Struktur der QES-Anwendung	72
Abbildung 4: Abb_HBA_ObjSys_004 Prinzipielle Struktur von DF.ESIGN	89
Abbildung 5: Abb_HBA_ObjSys_005 DF.CIA-Anwendungen und ihre Unterstrukturen ..	116
Abbildung 6: Abb_HBA_ObjSys_006 Prinzipielle Struktur von DF.AUTO	149
Abbildung 1: Abb_HBA_ObjSys_001 Allgemeine Dateistruktur eines HBA	25
Abbildung 2: Abb_HBA_ObjSys_002 Dateistruktur von DF.HPA	68
Abbildung 3: Abb_HBA_ObjSys_003 Prinzipielle Struktur der QES-Anwendung	72
Abbildung 4: Abb_HBA_ObjSys_004 Prinzipielle Struktur von DF.ESIGN	89
Abbildung 5: Abb_HBA_ObjSys_005 DF.CIA-Anwendungen und ihre Unterstrukturen ..	116
Abbildung 6: Abb_HBA_ObjSys_006 Prinzipielle Struktur von DF.AUTO	149

6.4 Tabellenverzeichnis

Tabelle 1: Tab_HBA_ObjSys_001 Liste der Komponenten, an welche dieses Dokument Anforderungen stellt	13
Tabelle 2: Tab_HBA_ObjSys_003 ATR-Kodierung (Sequenz von oben nach unten)	24
Tabelle 3: Tab_HBA_ObjSys_004 Initialisierte Attribute von MF	25
Tabelle 4: Tab_HBA_ObjSys_005 Initialisierte Attribute von MF / EF.ATR	27
Tabelle 5: Tab_HBA_ObjSys_083 Initialisierte Attribute von MF / EF.CardAccess	29
Tabelle 6: Tab_HBA_ObjSys_007 Initialisierte Attribute von MF / EF.DIR	31
Tabelle 7: Tab_HBA_ObjSys_008 Initialisierte Attribute von MF / EF.GDO	33
Tabelle 8: Tab_HBA_ObjSys_151 Personalisierte Attribute von MF / EF.GDO	34
Tabelle 9: Tab_HBA_ObjSys_009 Initialisierte Attribute von MF / EF.Version2	35
Tabelle 10: Tab_HBA_ObjSys_011 Initialisierte Attribute von MF / EF.C.CA_HPC.CS.E256	37
Tabelle 11: Tab_HBA_ObjSys_090 Personalisierte Attribute von MF / EF.C.CA_HPC.CS.E256	39

2626	Tabelle 12: Tab_HBA_ObjSys_014 Initialisierte Attribute von MF /	
2627	EF.C.HPC.AUTR_CVC.E256.....	39
2628	Tabelle 13: Tab_HBA_ObjSys_093 Personalisierte Attribute von MF /	
2629	EF.C.HPC.AUTR_CVC.E256.....	41
2630	Tabelle 14: Tab_HBA_ObjSys_017 Initialisierte Attribute von MF /	
2631	EF.C.HPC.AUTD_SUK_CVC.E256.....	42
2632	Tabelle 15: Tab_HBA_ObjSys_095 Personalisierte Attribute von MF /	
2633	EF.C.HPC.AUTD_SUK_CVC.E256.....	44
2634	Tabelle 16: Tab_HBA_ObjSys_019 Initialisierte Attribute von MF / PIN.CH.....	44
2635	Tabelle 17: Tab_HBA_ObjSys_097 Personalisierte Attribute von MF / PIN.CH.....	46
2636	Tabelle 18: Tab_HBA_ObjSys_021 Initialisierte Attribute von MF /	
2637	PrK.HPC.AUTR_CVC.E256.....	47
2638	Tabelle 19: Tab_HBA_ObjSys_099 Personalisierte Attribute von MF /	
2639	PrK.HPC.AUTR_CVC.E256.....	48
2640	Tabelle 20: Tab_HBA_ObjSys_024 Initialisierte Attribute von MF /	
2641	PrK.HPC.AUTD_SUK_CVC.E256.....	49
2642	Tabelle 21: Tab_HBA_ObjSys_101 Personalisierte Attribute von MF /	
2643	PrK.HPC.AUTD_SUK_CVC.E256.....	50
2644	Tabelle 22: Tab_HBA_ObjSys_027 Initialisierte Attribute von MF / PuK.RCA.CS.E256...51	
2645	Tabelle 23: Tab_HBA_ObjSys_153 Personalisierte Attribute von MF / PuK.RCA.CS.E256	
2646	für Testkarten.....	53
2647	Tabelle 24: Tab_HBA_ObjSys_082 Initialisierte Attribute von MF /	
2648	PuK.RCA.ADMINCMS.CS.E256.....	55
2649	Tabelle 25: Tab_HBA_ObjSys_103 Personalisierte Attribute von MF /	
2650	PuK.RCA.ADMINCMS.CS.E256.....	57
2651	Tabelle 26: Tab_HBA_ObjSys_029 Initialisierte Attribute von MF / SK.CMS.AES128.....58	
2652	Tabelle 27: Tab_HBA_ObjSys_104 Personalisierte Attribute von MF / SK.CMS.AES128..60	
2653	Tabelle 28: Tab_HBA_ObjSys_030 Initialisierte Attribute von MF / SK.CMS.AES256.....60	
2654	Tabelle 29: Tab_HBA_ObjSys_105 Personalisierte Attribute von MF / SK.CMS.AES256..61	
2655	Tabelle 30: Tab_HBA_ObjSys_147 Initialisierte Attribute von MF / SK.CUP.AES128.....62	
2656	Tabelle 31: Tab_HBA_ObjSys_148 Personalisierte Attribute von MF / SK.CUP.AES128..63	
2657	Tabelle 32: Tab_HBA_ObjSys_149 Initialisierte Attribute von MF / SK.CUP.AES256.....64	
2658	Tabelle 33: Tab_HBA_ObjSys_150 Personalisierte Attribute von MF / SK.CUP.AES256..65	
2659	Tabelle 34: Tab_HBA_ObjSys_076 Initialisierte Attribute von MF / SK.CAN.....66	
2660	Tabelle 35: Tab_HBA_ObjSys_106 Personalisierte Attribute von MF / SK.CAN.....67	
2661	Tabelle 36: Tab_HBA_ObjSys_031 Initialisierte Attribute von MF / DF.HPA.....68	
2662	Tabelle 37: Tab_HBA_ObjSys_032 Initialisierte Attribute von MF / DF.HPA / EF.HPD.....70	
2663	Tabelle 38: Tab_HBA_ObjSys_033 Initialisierte Attribute von MF / DF.QES.....72	
2664	Tabelle 39: Tab_HBA_ObjSys_034 Initialisierte Attribute von MF / DF.QES /	
2665	PrK.HP.QES.R2048.....	74

2666	Tabelle 40: Tab_HBA_ObjSys_108 Personalisierte Attribute von MF / DF.QES /	
2667	PrK.HP.QES.R2048	76
2668	Tabelle 41: Tab_HBA_ObjSys_037 Initialisierte Attribute von MF / DF.QES / PIN.QES ...	76
2669	Tabelle 42: Tab_HBA_ObjSys_111 Personalisierte Attribute von MF / DF.QES / PIN.QES	
2670	79
2671	Tabelle 43: Tab_HBA_ObjSys_038 Initialisierte Attribute von MF / DF.QES / EF.SSEC ...	79
2672	Tabelle 44: Tab_HBA_ObjSys_039 Inhalt von EF.SSEC.....	81
2673	Tabelle 45: Tab_HBA_ObjSys_040 Initialisierte Attribute von MF / DF.QES /	
2674	EF.C.HP.QES.R2048	82
2675	Tabelle 46: Tab_HBA_ObjSys_113 Personalisierte Attribute von MF / DF.QES /	
2676	EF.C.HP.QES.R2048	84
2677	Tabelle 47: Tab_HBA_ObjSys_160 Initialisierte Attribute MF / DF.QES / PrK.HP.QES.E256	
2678	85
2679	Tabelle 48: Tab_HBA_ObjSys_161 Personalisierte Attribute von MF / DF.QES /	
2680	PrK.HP.QES.E256	86
2681	Tabelle 49: Tab_HBA_ObjSys_162 Initialisierte Attribute von MF / DF.QES /	
2682	EF.C.HP.QES.E256	87
2683	Tabelle 50: Tab_HBA_ObjSys_045 Initialisierte Attribute von MF / DF.ESIGN	90
2684	Tabelle 51: Tab_HBA_ObjSys_046 Initialisierte Attribute von MF / DF.ESIGN /	
2685	PrK.HP.AUT.R2048	91
2686	Tabelle 52: Tab_HBA_ObjSys_118 Personalisierte Attribute von MF / DF.ESIGN /	
2687	PrK.HP.AUT.R2048	93
2688	Tabelle 53: Tab_HBA_ObjSys_049 Initialisierte Attribute von MF / DF.ESIGN /	
2689	PrK.HP.ENC.R2048	94
2690	Tabelle 54: Tab_HBA_ObjSys_121 Personalisierte Attribute von MF / DF.ESIGN /	
2691	PrK.HP.ENC.R2048	96
2692	Tabelle 55: Tab_HBA_ObjSys_055 Initialisierte Attribute von MF / DF.ESIGN /	
2693	EF.C.HP.AUT.R2048	96
2694	Tabelle 56: Tab_HBA_ObjSys_127 Personalisierte Attribute von MF / DF.ESIGN /	
2695	EF.C.HP.AUT.R2048	98
2696	Tabelle 57: Tab_HBA_ObjSys_056 Initialisierte Attribute von MF / DF.ESIGN /	
2697	EF.C.HP.ENC.R2048	98
2698	Tabelle 58: Tab_HBA_ObjSys_129 Personalisierte Attribute von MF / DF.ESIGN /	
2699	EF.C.HP.ENC.R2048	100
2700	Tabelle 59: Tab_HBA_ObjSys_170 Initialisierte Attribute von MF / DF.ESIGN /	
2701	PrK.HP.AUT.E256	100
2702	Tabelle 60: Tab_HBA_ObjSys_171 Personalisierte Attribute von MF / DF.ESIGN /	
2703	PrK.HP.AUT.E256	102
2704	Tabelle 61: Tab_HBA_ObjSys_172 Initialisierte Attribute von MF / DF.ESIGN /	
2705	PrK.HP.ENC.E256	103
2706	Tabelle 62: Tab_HBA_ObjSys_173 Personalisierte Attribute von MF / DF.ESIGN /	
2707	PrK.HP.ENC.E256	105

2708	Tabelle 63: Tab_HBA_ObjSys_174 Initialisierte Attribute von MF / DF.ESIGN /	
2709	EF.C.HP.AUT.E256	105
2710	Tabelle 64: Tab_HBA_ObjSys_175 Personalisierte Attribute von MF / DF.ESIGN /	
2711	EF.C.HP.AUT.E256	107
2712	Tabelle 65: Tab_HBA_ObjSys_176 Initialisierte Attribute von MF / DF.ESIGN /	
2713	EF.C.HP.ENC.E256	107
2714	Tabelle 66: Tab_HBA_ObjSys_177 Personalisierte Attribute von MF / DF.ESIGN /	
2715	EF.C.HP.ENC.E256	109
2716	Tabelle 67: Tab_HBA_ObjSys_130 initialisierte Attribute von MF / DF.ESIGN /	
2717	EF.C.HP.SIG.R2048	109
2718	Tabelle 68: Tab_HBA_ObjSys_136 Personalisierte Attribute von MF / DF.ESIGN /	
2719	EF.C.HP.SIG.R2048	111
2720	Tabelle 69: Tab_HBA_ObjSys_131 Initialisierte Attribute von MF / DF.ESIGN /	
2721	EF.C.HP.SIG.E256	111
2722	Tabelle 70: Tab_HBA_ObjSys_137 Personalisierte Attribute von MF / DF.ESIGN /	
2723	EF.C.HP.SIG.E256	112
2724	Tabelle 71: Tab_HBA_ObjSys_132 Initialisierte Attribute von MF / DF.ESIGN /	
2725	PrK.HP.SIG.R2048	113
2726	Tabelle 72: Tab_HBA_ObjSys_133 Personalisierte Attribute von MF / DF.ESIGN /	
2727	PrK.HP.SIG.R2048E256	114
2728	Tabelle 73: Tab_HBA_ObjSys_134 Initialisierte Attribute von MF / DF.ESIGN /	
2729	PrK.HP.SIG.E256	114
2730	Tabelle 74: Tab_HBA_ObjSys_135 Personalisierte Attribute von MF / DF.ESIGN /	
2731	PrK.HP.SIG.E256	115
2732	Tabelle 75: Tab_HBA_ObjSys_057 Initialisierte Attribute von MF / DF.CIA.QES	116
2733	Tabelle 76: Tab_HBA_ObjSys_059 Initialisierte Attribute von MF / DF.CIA.QES /	
2734	EF.CIA.CIAInfo (Cryptographic Information Application Info)	117
2735	Tabelle 77: Tab_HBA_ObjSys_060 Initialisierte Attribute von MF / DF.CIA.QES / EF.OD	
2736	120
2737	Tabelle 78: Tab_HBA_ObjSys_061 Initialisierte Attribute von MF / DF.CIA.QES / EF.AOD	
2738	(Authentication Object Directory)	122
2739	Tabelle 79: Tab_HBA_ObjSys_062 Initialisierte Attribute von MF / DF.CIA.QES / EF.PrKD	
2740	(Private Key Directory)	125
2741	Tabelle 80: Tab_HBA_ObjSys_063 Initialisierte Attribute von MF / DF.CIA.QES / EF.CD	
2742	(Certificate Directory)	128
2743	Tabelle 81: Tab_HBA_ObjSys_058 Initialisierte Attribute von MF / DF.CIA.ESIGN	130
2744	Tabelle 82: Tab_HBA_ObjSys_145 Initialisierte Attribute von MF / DF.CIA.ESIGN /	
2745	EF.CIA.CIAInfo (Cryptographic Information Application Info)	131
2746	Tabelle 83: Tab_HBA_ObjSys_146 Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.OD	
2747	(Object Directory)	135
2748	Tabelle 84: Tab_HBA_ObjSys_147 Initialisierte Attribute von MF / DF.CIA.ESIGN /	
2749	EF.AOD (Authentication Object Directory)	137

2750	Tabelle 85: Tab_HBA_ObjSys_148 Initialisierte Attribute von MF / DF.CIA.ESIGN /	
2751	EF.PrKD (Private Key Directory)	140
2752	Tabelle 86: Tab_HBA_ObjSys_149 Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.CD	
2753	(Certificate Directory)	145
2754	Tabelle 87: Tab_HBA_ObjSys_064 Initialisierte Attribute von MF / DF.AUTO	149
2755	Tabelle 88: Tab_HBA_ObjSys_065 Initialisierte Attribute von MF / DF.AUTO /	
2756	PrK.HP.AUTO.R3072	151
2757	Tabelle 89: Tab_HBA_ObjSys_138 Personalisierte Attribute von MF / DF.AUTO /	
2758	PrK.HP.AUTO.R3072	152
2759	Tabelle 90: Tab_HBA_ObjSys_068 Initialisierte Attribute von MF / DF.AUTO / PIN.AUTO	
2760	153
2761	Tabelle 91: Tab_HBA_ObjSys_141 Personalisierte Attribute von MF / DF.AUTO /	
2762	PIN.AUTO	156
2763	Tabelle 92: Tab_HBA_ObjSys_069 Initialisierte Attribute von MF / DF.AUTO / PIN.SO	156
2764	Tabelle 93: Tab_HBA_ObjSys_142 Personalisierte Attribute von MF / DF.AUTO / PIN.SO	
2765	159
2766	Tabelle 94: Tab_HBA_ObjSys_070 Initialisierte Attribute von MF / DF.AUTO /	
2767	EF.C.HP.AUTO1.R3072	159
2768	Tabelle 95: Tab_HBA_ObjSys_143 Personalisierte Attribute von MF / DF.AUTO /	
2769	EF.C.HP.AUTO1.R3072	161
2770	Tabelle 96: Tab_HBA_ObjSys_071 Initialisierte Attribute von MF / DF.AUTO /	
2771	EF.C.HP.AUTO2.R3072	162
2772	Tabelle 97: Tab_HBA_ObjSys_144 Personalisierte Attribute von MF / DF.AUTO /	
2773	EF.C.HP.AUTO2.R3072	163
2774	Tabelle 1: Tab_HBA_ObjSys_001 Liste der Komponenten, an welche dieses Dokument	
2775	Anforderungen stellt	13
2776	Tabelle 2: Tab_HBA_ObjSys_003 ATR-Kodierung (Sequenz von oben nach unten).....	24
2777	Tabelle 3: Tab_HBA_ObjSys_004 Initialisierte Attribute von MF	25
2778	Tabelle 4: Tab_HBA_ObjSys_005 Initialisierte Attribute von MF / EF.ATR	27
2779	Tabelle 5: Tab_HBA_ObjSys_083 Initialisierte Attribute von MF / EF.CardAccess	29
2780	Tabelle 6: Tab_HBA_ObjSys_007 Initialisierte Attribute von MF / EF.DIR	31
2781	Tabelle 7: Tab_HBA_ObjSys_008 Initialisierte Attribute von MF / EF.GDO	33
2782	Tabelle 8: Tab_HBA_ObjSys_151 Personalisierte Attribute von MF / EF.GDO	34
2783	Tabelle 9: Tab_HBA_ObjSys_009 Initialisierte Attribute von MF / EF.Version2	35
2784	Tabelle 10: Tab_HBA_ObjSys_011 Initialisierte Attribute von MF / EF.C.CA HPC.CS.E256	
2785	37
2786	Tabelle 11: Tab_HBA_ObjSys_090 Personalisierte Attribute von MF /	
2787	EF.C.CA HPC.CS.E256	39
2788	Tabelle 12: Tab_HBA_ObjSys_014 Initialisierte Attribute von MF /	
2789	EF.C.HPC.AUTR CVC.E256	39

2790	Tabelle 13: Tab HBA_ObjSys_093 Personalisierte Attribute von MF /	
2791	EF.C.HPC.AUTR CVC.E256.....	41
2792	Tabelle 14: Tab HBA_ObjSys_017 Initialisierte Attribute von MF /	
2793	EF.C.HPC.AUTD SUK CVC.E256.....	42
2794	Tabelle 15: Tab HBA_ObjSys_095 Personalisierte Attribute von MF /	
2795	EF.C.HPC.AUTD SUK CVC.E256.....	44
2796	Tabelle 16: Tab HBA_ObjSys_019 Initialisierte Attribute von MF / PIN.CH.....	44
2797	Tabelle 17: Tab HBA_ObjSys_097 Personalisierte Attribute von MF / PIN.CH.....	46
2798	Tabelle 18: Tab HBA_ObjSys_021 Initialisierte Attribute von MF /	
2799	PrK.HPC.AUTR CVC.E256.....	47
2800	Tabelle 19: Tab HBA_ObjSys_099 Personalisierte Attribute von MF /	
2801	PrK.HPC.AUTR CVC.E256.....	48
2802	Tabelle 20: Tab HBA_ObjSys_024 Initialisierte Attribute von MF /	
2803	PrK.HPC.AUTD SUK CVC.E256.....	49
2804	Tabelle 21: Tab HBA_ObjSys_101 Personalisierte Attribute von MF /	
2805	PrK.HPC.AUTD SUK CVC.E256.....	50
2806	Tabelle 22: Tab HBA_ObjSys_027 Initialisierte Attribute von MF / PuK.RCA.CS.E256...	51
2807	Tabelle 23: Tab HBA_ObjSys_153 Personalisierte Attribute von MF / PuK.RCA.CS.E256	
2808	für Testkarten.....	53
2809	Tabelle 24: Tab HBA_ObjSys_082 Initialisierte Attribute von MF /	
2810	PuK.RCA.ADMINCMS.CS.E256.....	55
2811	Tabelle 25: Tab HBA_ObjSys_103 Personalisierte Attribute von MF /	
2812	PuK.RCA.ADMINCMS.CS.E256.....	57
2813	Tabelle 26: Tab HBA_ObjSys_029 Initialisierte Attribute von MF / SK.CMS.AES128.....	58
2814	Tabelle 27: Tab HBA_ObjSys_104 Personalisierte Attribute von MF / SK.CMS.AES128 ..	60
2815	Tabelle 28: Tab HBA_ObjSys_030 Initialisierte Attribute von MF / SK.CMS.AES256.....	60
2816	Tabelle 29: Tab HBA_ObjSys_105 Personalisierte Attribute von MF / SK.CMS.AES256 ..	61
2817	Tabelle 30: Tab HBA_ObjSys_147 Initialisierte Attribute von MF / SK.CUP.AES128.....	62
2818	Tabelle 31: Tab HBA_ObjSys_148 Personalisierte Attribute von MF / SK.CUP.AES128 ..	63
2819	Tabelle 32: Tab HBA_ObjSys_149 Initialisierte Attribute von MF / SK.CUP.AES256.....	64
2820	Tabelle 33: Tab HBA_ObjSys_150 Personalisierte Attribute von MF / SK.CUP.AES256 ..	65
2821	Tabelle 34: Tab HBA_ObjSys_076 Initialisierte Attribute von MF / SK.CAN.....	66
2822	Tabelle 35: Tab HBA_ObjSys_106 Personalisierte Attribute von MF / SK.CAN.....	67
2823	Tabelle 36: Tab HBA_ObjSys_031 Initialisierte Attribute von MF / DF.HPA.....	68
2824	Tabelle 37: Tab HBA_ObjSys_032 Initialisierte Attribute von MF / DF.HPA / EF.HPD.....	70
2825	Tabelle 38: Tab HBA_ObjSys_033 Initialisierte Attribute von MF / DF.QES.....	72
2826	Tabelle 39: Tab HBA_ObjSys_034 Initialisierte Attribute von MF / DF.QES /	
2827	PrK.HP.QES.R2048.....	74
2828	Tabelle 40: Tab HBA_ObjSys_108 Personalisierte Attribute von MF / DF.QES /	
2829	PrK.HP.QES.R2048.....	76

2830	Tabelle 41: Tab HBA ObjSys 037 Initialisierte Attribute von MF / DF.QES / PIN.QES ...	76
2831	Tabelle 42: Tab HBA ObjSys 111 Personalisierte Attribute von MF / DF.QES / PIN.QES	
2832	79
2833	Tabelle 43: Tab HBA ObjSys 038 Initialisierte Attribute von MF / DF.QES / EF.SSEC ...	79
2834	Tabelle 44: Tab HBA ObjSys 039 Inhalt von EF.SSEC.....	81
2835	Tabelle 45: Tab HBA ObjSys 040 Initialisierte Attribute von MF / DF.QES /	
2836	EF.C.HP.QES.R2048.....	82
2837	Tabelle 46: Tab HBA ObjSys 113 Personalisierte Attribute von MF / DF.QES /	
2838	EF.C.HP.QES.R2048.....	84
2839	Tabelle 47: Tab HBA ObjSys 160 Initialisierte Attribute MF / DF.QES / PrK.HP.QES.E256	
2840	85
2841	Tabelle 48: Tab HBA ObjSys 161 Personalisierte Attribute von MF / DF.QES /	
2842	PrK.HP.QES.E256	86
2843	Tabelle 49: Tab HBA ObjSys 162 Initialisierte Attribute von MF / DF.QES /	
2844	EF.C.HP.QES.E256.....	87
2845	Tabelle 50: Tab HBA ObjSys 045 Initialisierte Attribute von MF / DF.ESIGN	90
2846	Tabelle 51: Tab HBA ObjSys 046 Initialisierte Attribute von MF / DF.ESIGN /	
2847	PrK.HP.AUT.R2048	91
2848	Tabelle 52: Tab HBA ObjSys 118 Personalisierte Attribute von MF / DF.ESIGN /	
2849	PrK.HP.AUT.R2048	93
2850	Tabelle 53: Tab HBA ObjSys 049 Initialisierte Attribute von MF / DF.ESIGN /	
2851	PrK.HP.ENC.R2048	94
2852	Tabelle 54: Tab HBA ObjSys 121 Personalisierte Attribute von MF / DF.ESIGN /	
2853	PrK.HP.ENC.R2048	96
2854	Tabelle 55: Tab HBA ObjSys 055 Initialisierte Attribute von MF / DF.ESIGN /	
2855	EF.C.HP.AUT.R2048	96
2856	Tabelle 56: Tab HBA ObjSys 127 Personalisierte Attribute von MF / DF.ESIGN /	
2857	EF.C.HP.AUT.R2048	98
2858	Tabelle 57: Tab HBA ObjSys 056 Initialisierte Attribute von MF / DF.ESIGN /	
2859	EF.C.HP.ENC.R2048	98
2860	Tabelle 58: Tab HBA ObjSys 129 Personalisierte Attribute von MF / DF.ESIGN /	
2861	EF.C.HP.ENC.R2048	100
2862	Tabelle 59: Tab HBA ObjSys 170 Initialisierte Attribute von MF / DF.ESIGN /	
2863	PrK.HP.AUT.E256	100
2864	Tabelle 60: Tab HBA ObjSys 171 Personalisierte Attribute von MF / DF.ESIGN /	
2865	PrK.HP.AUT.E256	102
2866	Tabelle 61: Tab HBA ObjSys 172 Initialisierte Attribute von MF / DF.ESIGN /	
2867	PrK.HP.ENC.E256	103
2868	Tabelle 62: Tab HBA ObjSys 173 Personalisierte Attribute von MF / DF.ESIGN /	
2869	PrK.HP.ENC.E256	105
2870	Tabelle 63: Tab HBA ObjSys 174 Initialisierte Attribute von MF / DF.ESIGN /	
2871	EF.C.HP.AUT.E256	105

2872	Tabelle 64: Tab HBA_ObjSys_175 Personalisierte Attribute von MF / DF.ESIGN /	
2873	EF.C.HP.AUT.E256	107
2874	Tabelle 65: Tab HBA_ObjSys_176 Initialisierte Attribute von MF / DF.ESIGN /	
2875	EF.C.HP.ENC.E256	107
2876	Tabelle 66: Tab HBA_ObjSys_177 Personalisierte Attribute von MF / DF.ESIGN /	
2877	EF.C.HP.ENC.E256	109
2878	Tabelle 67: Tab HBA_ObjSys_130 initialisierte Attribute von MF / DF.ESIGN /	
2879	EF.C.HP.SIG.R2048	109
2880	Tabelle 68: Tab HBA_ObjSys_136 Personalisierte Attribute von MF / DF.ESIGN /	
2881	EF.C.HP.SIG.R2048	111
2882	Tabelle 69: Tab HBA_ObjSys_131 Initialisierte Attribute von MF / DF.ESIGN /	
2883	EF.C.HP.SIG.E256	111
2884	Tabelle 70: Tab HBA_ObjSys_137 Personalisierte Attribute von MF / DF.ESIGN /	
2885	EF.C.HP.SIG.E256	112
2886	Tabelle 71: Tab HBA_ObjSys_132 Initialisierte Attribute von MF / DF.ESIGN /	
2887	PrK.HP.SIG.R2048	113
2888	Tabelle 72: Tab HBA_ObjSys_133 Personalisierte Attribute von MF / DF.ESIGN /	
2889	PrK.HP.SIG.R2048E256	114
2890	Tabelle 73: Tab HBA_ObjSys_134 Initialisierte Attribute von MF / DF.ESIGN /	
2891	PrK.HP.SIG.E256	114
2892	Tabelle 74: Tab HBA_ObjSys_135 Personalisierte Attribute von MF / DF.ESIGN /	
2893	PrK.HP.SIG.E256	115
2894	Tabelle 75: Tab HBA_ObjSys_057 Initialisierte Attribute von MF / DF.CIA.QES	116
2895	Tabelle 76: Tab HBA_ObjSys_059 Initialisierte Attribute von MF / DF.CIA.QES /	
2896	EF.CIA.CIAInfo (Cryptographic Information Application Info)	117
2897	Tabelle 77: Tab HBA_ObjSys_060 Initialisierte Attribute von MF / DF.CIA.QES / EF.OD	
2898	120
2899	Tabelle 78: Tab HBA_ObjSys_061 Initialisierte Attribute von MF / DF.CIA.QES / EF.AOD	
2900	(Authentication Object Directory)	122
2901	Tabelle 79: Tab HBA_ObjSys_062 Initialisierte Attribute von MF / DF.CIA.QES / EF.PrKD	
2902	(Private Key Directory)	125
2903	Tabelle 80: Tab HBA_ObjSys_063 Initialisierte Attribute von MF / DF.CIA.QES / EF.CD	
2904	(Certificate Directory)	128
2905	Tabelle 81: Tab HBA_ObjSys_058 Initialisierte Attribute von MF / DF.CIA.ESIGN	130
2906	Tabelle 82: Tab HBA_ObjSys_145 Initialisierte Attribute von MF / DF.CIA.ESIGN /	
2907	EF.CIA.CIAInfo (Cryptographic Information Application Info)	131
2908	Tabelle 83: Tab HBA_ObjSys_146 Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.OD	
2909	(Object Directory)	135
2910	Tabelle 84: Tab HBA_ObjSys_147 Initialisierte Attribute von MF / DF.CIA.ESIGN /	
2911	EF.AOD (Authentication Object Directory)	137
2912	Tabelle 85: Tab HBA_ObjSys_148 Initialisierte Attribute von MF / DF.CIA.ESIGN /	
2913	EF.PrKD (Private Key Directory)	140

Tabelle 86: Tab HBA_ObjSys_149 Initialisierte Attribute von MF / DF.CIA.ESIGN / EF.CD (Certificate Directory)	145
Tabelle 87: Tab HBA_ObjSys_064 Initialisierte Attribute von MF / DF.AUTO	149
Tabelle 88: Tab HBA_ObjSys_065 Initialisierte Attribute von MF / DF.AUTO / PrK.HP.AUTO.R3072	151
Tabelle 89: Tab HBA_ObjSys_138 Personalisierte Attribute von MF / DF.AUTO / PrK.HP.AUTO.R3072	152
Tabelle 90: Tab HBA_ObjSys_068 Initialisierte Attribute von MF / DF.AUTO / PIN.AUTO	153
Tabelle 91: Tab HBA_ObjSys_141 Personalisierte Attribute von MF / DF.AUTO / PIN.AUTO	156
Tabelle 92: Tab HBA_ObjSys_069 Initialisierte Attribute von MF / DF.AUTO / PIN.SO	156
Tabelle 93: Tab HBA_ObjSys_142 Personalisierte Attribute von MF / DF.AUTO / PIN.SO	159
Tabelle 94: Tab HBA_ObjSys_070 Initialisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO1.R3072	159
Tabelle 95: Tab HBA_ObjSys_143 Personalisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO1.R3072	161
Tabelle 96: Tab HBA_ObjSys_071 Initialisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO2.R3072	162
Tabelle 97: Tab HBA_ObjSys_144 Personalisierte Attribute von MF / DF.AUTO / EF.C.HP.AUTO2.R3072	163

6.5 Referenzierte Dokumente

6.5.1 Dokumente der gematik

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

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[gemSpec_COS]	gematik: Spezifikation COS - Spezifikation der elektrischen Schnittstelle
[gemSpec_Karten_Fach_TIP_G2.1]	gematik: Befüllvorschriften für die Plattformanteile der Karten der TI der Generation G2.1

[gemSpec_PINPUK_TI]	gematik: Übergreifende Spezifikation PIN/PUK-Policy für Smartcards der Telematikinfrastruktur
[gemSpec_CAN_TI]	gematik: Übergreifende Spezifikation CAN-Policy
[gemSpec_Krypt]	gematik: Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_OID]	gematik: Spezifikation Festlegung von OIDs
[gemSpec_PKI]	gematik: Übergreifende Spezifikation Spezifikation PKI
[gemSpec_CVC_Root]	gematik: Spezifikation CVC - Root
[gemSpec_CVC_TSP]	gematik: Spezifikation Trust Service Provider CVC
[gemSpec_TK]	gematik: Spezifikation für Testkarten gematik (eGK, HBA, (g)SMC) der Generation 2

2945 6.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[ALGCAT]	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen: Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) in der aktuellen Fassung, siehe www.bundesnetzagentur.de
[DIN66291-1]	DIN V66291-1: 2000 Chipkarten mit Digitaler Signatur-Anwendung/Funktion nach SigG und SigV, Teil 1: Anwendungsschnittstelle
[EN14890-1]	EN 14890-1: 2008 Application Interface for smart cards used as secure signature creation devices, Part 1: Basic services
[EN1867]	EN 1867:1997 Machine readable cards – Health care applications – Numbering system and registration procedure for issuer identifiers
[ISO3166-1]	ISO/IEC 3166-1: 2006 Codes for the representations of names of countries and their subdivisions – Part 1: Country codes

[ISO7816-3]	ISO/IEC 7816-3: 2006 Identification cards - Integrated circuit cards with contacts - Part 3: Electrical interface and transmission protocols
[ISO7816-4]	ISO/IEC 7816-4: 2005 Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange
[ISO7816-15]	ISO/IEC 7816-15: 2016 Identification cards - Integrated circuit cards - Part 15: Cryptographic information application
[ISO8825-1]	ISO/IEC 8825-1: 2002 Information technology - ASN.1 encoding rules - Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)
[PKCS#1]	RSA Laboratories (June 14, 2002): RSA Cryptography Standard v2.1 (earlier versions: V1.5: Nov. 1993, V2.0: July, 1998)
[Beschluss 190]	Beschluss Nr. 190 der Europäischen Union vom 18. Juni 2003 betreffend die technischen Merkmale der europäischen Krankenversicherungskarte
[RFC2119]	Network Working Group, Request for Comments: 2119, S. Bradner Harvard, University, March 1997, Category: Best Current Practice Key words for use in RFCs to Indicate Requirement Level http://tools.ietf.org/html/rfc2119
[RSA]	R. Rivest, A. Shamir, L. Adleman: A method for obtaining digital signatures and public key cryptosystems, Communications of the ACM, Vol. 21 No. 2, 1978
[SD5]	ISO/IEC JTC1/SC17 STANDING DOCUMENT 5, 2006-06-19 Register of IC manufacturers http://www.pkicc.de/cms/media/pdfs/IC_manufacturer_ISO_SD5_1962006.pdf
[TR-03110-2]	Technical Guideline TR-03110-2 Advanced Security Mechanisms for Machine Readable Travel Documents – Part 2 – Extended Access Control Version 2 (EACv2), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI) Version 2.10 vom 20.3.2012
[TR-03114]	BSI: TR 03114, Stapelsignatur mit dem Heilberufsausweis, Version 2.0, 22.10.2007

[TR-03115]	BSI: TR-03115, Komfortsignatur mit dem Heilberufsausweis, Version 2.0, 19.10.2007
[TR-03116-1]	Technische Richtlinie BSI TR-03116-1 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 1: Telematikinfrastruktur, Version 3.18 vom 30.01.2014

2946

ENTWURF