

Spezifikation des elektronischen Heilberufsausweises

Teil III: SMC - Anwendungen und Funktionen

Version 2.3.2

05.08.2009

Bundesärztekammer

Kassenärztliche Bundesvereinigung

Bundeszahnärztekammer

Bundespsychotherapeutenkammer

Kassenzahnärztliche Bundesvereinigung

Bundesapothekerkammer

Deutsche Krankenhausgesellschaft

Editor: Ulrich Waldmann (Fraunhofer-Institut SIT)

Die technische Spezifikation für den Heilberufsausweis (HPC) und die Sicherheitsmodulkarte (SMC) besteht aus folgenden Teilen:

Teil 1: Kommandos, Algorithmen und Funktionen der Betriebssystemplattform

Teil 2: HPC – Anwendungen und Funktionen

Teil 3: SMC – Anwendungen und Funktionen

Inhaltsverzeichnis

Inhaltsverzeichnis.....	3
1 Zielsetzung und Geltungsbereich.....	6
2 Referenzierte Dokumente	7
3 Abkürzungen	11
3.1 Abkürzungen	11
3.2 Notation	15
4 Typen von Sicherheitsmodulkarten.....	17
5 Sicherheitsmodulkarte A	18
5.1 ATR-Kodierung und technische Eigenschaften.....	18
5.2 Allgemeine Struktur	18
5.3 Root-Anwendung und Dateien auf MF-Ebene.....	19
5.3.1 MF	19
5.3.2 EF.ATR.....	19
5.3.3 EF.DIR.....	21
5.3.4 EF.GDO.....	22
5.3.5 EF.Version.....	23
5.3.6 EF.C.CA_SMC.CS	24
5.3.7 EF.C.SMC.AUTR_CVC.....	25
5.3.8 EF.C.SMC.AUTD_RPS_CVC	25
5.3.9 PrK.SMC.AUTR_CVC.....	26
5.3.10 PrK.SMC.AUTD_RPS_CVC.....	26
5.3.11 PuK.RCA.CS	27
5.3.12 PuK.CAMS_SMC.AUT_CVC	27
5.3.13 SK.CAMS	28
5.4 Sicherheitsumgebungen auf MF-Ebene	28
5.5 Öffnen der SMC-A	28
5.5.1 Auswahl der Root-Anwendung.....	28
5.5.2 Lesen von EF.ATR und EF.GDO	29
5.5.3 Lesen von EF.DIR und EF.Version	29
5.5.4 Lesen der zur SMC-A gehörenden CV Zertifikate.....	29
5.6 Management von Kanälen.....	29
5.7 Autorisierung der SMC-A.....	30
5.8 Interaktionen zwischen SMC-A und eGK	31
5.8.1 Asymmetrische SMC/eGK-Authentisierung ohne Aufbau eines Trusted Channel	31
5.8.2 Asymmetrische SMC/eGK-Authentisierung mit Aufbau eines Trusted Channel	31
5.9 Interaktionen zwischen SMC-A und HPC, SMC-B oder RFID-Token.....	32
5.9.1 Allgemeines.....	32
5.9.2 Asymmetrische Authentisierung mit Aufbau eines Trusted Channel	32
5.9.3 Asymmetrische Authentisierung mit Speicherung von Vorstellungsschlüsseln	34
5.9.4 Symmetrische Authentisierung mit Aufbau eines Trusted Channel.....	37
5.9.5 Erzeugen gesicherter Kommandos mit PSO-Kommandos	38
5.9.6 Verarbeiten gesicherter Antworten mit PSO-Kommandos.....	40
5.9.7 Erzeugen gesicherter Kommandos mit ENVELOPE (optional)	40
5.9.8 Verarbeiten gesicherter Antworten mit ENVELOPE (optional)	41
5.10 Die Sicherheitsmodul-Anwendung	42
5.10.1 Dateistruktur und Dateiinhalt	42
5.10.1.1 DF.SMA (Security Module Application)	42
5.10.1.2 EF.SMD	43
5.10.2 Sicherheitsumgebungen auf DF-Ebene	44
5.10.3 Auswahl der Anwendung.....	44
5.10.4 Lesen, Aktualisieren und Löschen von Daten in EF.SMD	44
5.11 Die KT-Anwendung (Kartenterminal-Anwendung).....	46
5.11.1 Dateistruktur und Dateiinhalt.....	46

5.11.1.1	DF.KT (Kartenterminal-Anwendung)	46
5.11.1.2	EF.C.SMKT.CA.....	47
5.11.1.3	EF.C.SMKT.AUT	47
5.11.1.4	PrK.SMKT.AUT.....	47
5.11.2	Sicherheitsumgebungen auf DF-Ebene	48
5.11.3	Auswahl der Anwendung.....	48
5.11.4	Lesen der X.509-Zertifikate	48
5.11.5	Generierung einer Zufallszahl	49
5.11.6	Verwendung des privaten Schlüssels	49
5.12	Laden einer neuen Anwendung oder Anlegen eines EFs nach Ausgabe der SMC-A	51
6	Sicherheitsmodulkarte B	52
6.1	ATR-Kodierung und technische Eigenschaften	52
6.2	Allgemeine Struktur	52
6.3	Root-Anwendung und Dateien auf MF-Ebene.....	53
6.3.1	MF	53
6.3.2	EF.ATR.....	54
6.3.3	EF.DIR.....	54
6.3.4	EF.GDO.....	55
6.3.5	EF.Version.....	55
6.3.6	EF.C.CA_SMC.CS	55
6.3.7	EF.C.SMC.AUTR_CVC.....	55
6.3.8	EF.C.SMC.AUTD_RPS_CVC	55
6.3.9	EF.C.SMC.AUTD_RPE_CVC	55
6.3.10	PIN.SMC.....	56
6.3.11	PrK.SMC.AUTR_CVC	56
6.3.12	PrK.SMC.AUTD_RPS_CVC.....	57
6.3.13	PrK.SMC.AUTD_RPE_CVC.....	58
6.3.14	PuK.RCA.CS	58
6.3.15	PuK.CAMS_SMC.AUT_CVC	58
6.3.16	SK.CAMS	58
6.4	Sicherheitsumgebungen auf MF-Ebene	59
6.5	Öffnen der SMC-B	59
6.5.1	Auswahl der Root-Anwendung.....	59
6.5.2	Lesen EF.ATR und EF.GDO	60
6.5.3	Lesen EF.DIR und EF.Version	60
6.5.4	Lesen der CV-Zertifikate der SMC-B	60
6.6	Management von Kanälen.....	60
6.7	Autorisierung der SMC-B.....	60
6.8	Interaktionen zwischen SMC-B und eGK	60
6.9	Interaktionen zwischen SMC-B und SMC-A oder RFID-Token	61
6.9.1	Allgemeines.....	61
6.9.2	Asymmetrische Authentisierung mit TC-Aufbau als PIN-Sender.....	61
6.9.3	Asymmetrische Authentisierung mit Speicherung von Vorstellungsschlüsseln als PIN-Sender	61
6.9.4	Asymmetrische Authentisierung mit TC-Aufbau als PIN-Empfänger.....	61
6.9.5	Asymmetrische Authentisierung mit Speicherung von Vorstellungsschlüsseln als PIN-Empfänger	61
6.9.6	Symmetrische Authentisierung als PIN-Sender	62
6.9.7	Symmetrische Authentisierung als PIN-Empfänger	62
6.10	Die Sicherheitsmodul-Anwendung	62
6.10.1	Dateistruktur und Dateinhalt.....	62
6.10.2	DF.SMA (Security Module Application).....	62
6.10.2.1	EF.SMD	63
6.10.2.2	EF.CONF	63
6.10.2.3	EF.NET	64
6.10.2.4	PIN.CONF.....	64
6.10.3	Auswahl der Anwendung.....	65
6.10.4	Lesen, Aktualisieren und Löschen von Daten in EF.SMD, EF.CONF und EF.NET	66
6.11	Die ESIGN-Anwendung	66

6.11.1	Dateistruktur und Dateiinhalt.....	66
6.11.2	DF.ESIGN (ESIGN-Anwendung).....	67
6.11.3	EF.C.HCI.OSIG	68
6.11.4	EF.C.HCI.AUT	68
6.11.5	EF.C.HCI.ENC.....	69
6.11.6	PrK.HCI.OSIG	69
6.11.7	PrK.HCI.AUT	69
6.11.8	PrK.HCI.ENC.....	70
6.11.9	Lesen der X.509-Zertifikate.....	70
6.11.10	Nutzen der privaten Schlüssel.....	71
6.12	Die Kartenterminal-Anwendung.....	71
6.13	Laden einer neuen Anwendung oder Anlegen eines EFs nach Ausgabe der SMC-B	71

1 Zielsetzung und Geltungsbereich

Dieser Teil der Spezifikation definiert die Kartenschnittstelle zu den

- Sicherheitsmodulkarten SMC-A und SMC-B zur Nutzung im Gesundheitswesen.

SMC-A und SMC-B bieten folgende Möglichkeiten:

- C2C-Authentisierung SMC/eGK,
- Unterstützung des Trusted Channel, d.h. Berechnung, Entschlüsselung und Prüfung von Secure Messaging Datenobjekten als entfernter PIN-Sender, der die gesicherte PIN-Übertragung zu einer PIN empfangenden Karte (HPC, RFID-Token oder SMC-B) ermöglicht. Dies kann in zukünftigen Anwendungen auch zur gesicherten Übertragung anderer Daten verwendet werden.
- Unterstützung der Authentisierung des Kartenterminals gegenüber dem Konnektor.

Die SMC-B unterstützt zusätzlich folgende Dienste:

- Organisationssignaturen für die beteiligten Institutionen des Gesundheitswesens
- Client/Server-Authentisierung für die beteiligten Institutionen des Gesundheitswesens
- Verschlüsselungsmöglichkeiten für die beteiligten Institutionen des Gesundheitswesens, so dass verschlüsselte Dokumente durch autorisierte Mitarbeiter der jeweiligen Institution des Gesundheitswesens entschlüsselt werden können,
- Unterstützung des Trusted Channel als entfernter PIN-Empfänger, der Secure Messaging Kommandos ausführt,
- Unterstützung der Konnektorwartung durch Speicherung von entsprechenden Konfigurationsdaten.

Die SMCs werden in Kartenterminals des Gesundheitswesens eingesetzt.

2 Referenzierte 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) vom 17. November 2008, siehe www.bundesnetzagentur.de
[COM-PKI-1]	T7, TeleTrusT: Common PKI Specification, Part 1: Certificate and CRL Profiles, Version 2.0, 20 th January 2009, www.common-pki.org
[COM-PKI-9]	T7, TeleTrusT: Common PKI Specification, Part 9: SigG-Profile, Version 2.0, 20th January 2009, www.common-pki.org
[DIN66291-1]	DIN V66291-1: 2000 Chipkarten mit Digitaler Signatur-Anwendung/Funktion nach SigG und SigV, Teil 1: Anwendungsschnittstelle
[DIN66291-4]	DIN V66291-4: 2002 Chipkarten mit Digitaler Signatur-Anwendung/Funktion nach SigG/SigV, Teil 4: Grundlegende Sicherheitsdienste
[ECDIR]	Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures
[eGK-P1]	gematik (2008): Spezifikation der elektronischen Gesundheitskarte, Teil 1: Spezifikation der elektrischen Schnittstelle, Version 2.2.2, 16.09.2008
[eGK-P2]	gematik (2008): Spezifikation der elektronischen Gesundheitskarte, Teil 2: Grundlegende Applikationen, Version 2.2.1, 19.06.2008
[EN14890-1]	EN 14890-1: 2008 Application Interface for smart cards used as secure signature creation devices, Part 1: Basic services
[EN14890-2]	EN 14890-2: 2008 Application Interface for smart cards used as Secure Signature Creation Devices, Part 2: Additional services
[EN1867]	EN 1867:1997 Machine readable cards – Health care applications – Numbering system and registration procedure for issuer identifiers
[GMG]	Gesetz zur Modernisierung der gesetzlichen Krankenversicherung (GKV-Modernisierungsgesetz - GMG), BGBl 2003 Teil I Nr. 55 S.2190, 19. November 2003
[HPC-P1]	Bundesärztekammer et al. Spezifikation des elektronischen Heilberufsausweises und der Security Module Card, Teil I: Kommandos, Algorithmen und Funktionen der Betriebssystemplattform, V2.3.2 DE, 05.08.2009
[HPC-P2]	Bundesärztekammer et al. Spezifikation des elektronischen Heilberufsausweises und der Security Module Card, Teil II: HPC – Anwendungen und Funktionen, V2.3.2 DE, 0.5.08.2009
[ISO3166]	ISO/IEC 3166-1: 2006 Codes for the representations of names of countries and their subdivisions

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
	– Part 1: Country codes
[ISO7812]	ISO/IEC 7812-1: 2006 Cards and personal identification – Identification of issuers – Part 1: Numbering system
[ISO7816-1]	ISO/IEC 7816-1: 1998 Identification cards - Integrated circuit cards with contacts - Part 1: Physical characteristics
[ISO7816-2]	ISO/IEC 7816-2: 2007 Identification cards - Integrated circuit cards with contacts - Part 2: Dimensions and location von contacts
[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
[ISO7816-5]	ISO/IEC 7816-5: 2004 Identification cards - Integrated circuit cards - Part 5: Registration of application providers
[ISO7816-6]	ISO/IEC 7816-6: 2004 Identification cards - Integrated circuit cards - Part 6: Interindustry data elements for interchange
[ISO7816-8]	ISO/IEC 7816-8: 2004 Identification cards - Integrated circuit cards - Part 8: Commands for security operations
[ISO7816-9]	ISO/IEC 7816-9: 2004 Identification cards - Integrated circuit cards - Part 9: Commands for card management
[ISO7816-13]	ISO/IEC 7816-13: 2007 Identification cards - Integrated circuit cards - Part 13: Commands for application management in multi-application environment
[ISO7816-15]	ISO/IEC 7816-15: 2004 Identification cards - Integrated circuit cards - Part 15: Cryptographic information application
[ISO8825]	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)
[ISO9564]	ISO 9564-1: 2002 Banking – Personal Identification Number (PIN) management and security, Part 1: Basic principles and requirements for online PIN handling in ATM and POS systems.
[ISO9796-2]	ISO 9796-2: 2002 Information technology – Security techniques – Digital signature schemes giving Message Recovery – Part 2: Integer factorization based mechanisms

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[ISO10118]	ISO 10118-2 Information technology – Security techniques – Hash functions, Part 2: Hash functions using an n-Bit block cipher algorithm, 2000
[ISO10646]	ISO/IEC 10646:2003 Information technology -- Universal Multiple-Octet Coded Character Set (UCS)
[ISO10918]	ISO/IEC 10918-1 Information technology - digital compression and coding of continuous-tone still images: Requirements and guidelines, 1994
[ISO11770]	ISO/IEC 11770-3: 2008 Information technology - Security techniques - Key management Part 3: Mechanisms using asymmetric techniques
[NIST-SHS]	NIST: FIPS Publication 180-2: Secure Hash Standard (SHS-1), 01.08.2002
[PKCS#1]	PKCS #1 RSA Cryptography Standard V2.1: June 14, 2002
[PKI-Reg]	gematik: Registrierung einer CVC-CA der zweiten Ebene Version 1.8.0
[PKI-Nota]	gematik: Festlegungen zu den Notationen von Schlüsseln und Zertifikaten kryptographischer Objekte in der TI, Version 1.1.0
[PP-HPC]	BSI: Common Criteria Protection Profile – Health Professional Card (PP-HPC) with SSCD Functionality, BSI-PP-0018, Version 1.3, February 1 st 2008
[PP-SMC-A]	BSI: Common Criteria Protection Profile – Secure Module Card Type A (PP-SMC-A), BSI-PP-0019, Version 1.9.1, February 1 st 2008
[PP-SMC-B]	BSI: Common Criteria Protection Profile – Secure Module Card Type B (PP-SMC-B), BSI-PP-0019, Version 1.9.1, February 1 st 2008
[Resolution190]	Beschluss Nr. 190 der Europäischen Union vom 18. Juni 2003 betreffend die technischen Merkmale der europäischen Krankenversicherungskarte
[RFC1510]	RFC 1510: May 1999 Public Key Cryptography for Initial Authentication in Kerberos
[RFC2246]	RFC 2246: Jan. 1999 The TLS Protocol, Version 1.0
[RFC2459]	Internet X.509 Public Key Infrastructure - Certificate and CRL Profile, January 1999
[RFC3039]	Internet X.509 Public Key Infrastructure Qualified Certificates Profile, January 2001
[RFC3280]	Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile, April 2002
[RFC3629]	UTF-8, a transformation format of ISO 10646, November 2003
[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
[SigG01]	Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften, Bundesgesetzblatt Nr. 22, 2001, S.876
[SigV01]	Verordnung zur elektronischen Signatur – SigV, 2001, Bundesgesetzblatt

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
	Nr. 509, 2001, S. 3074
[SMC-K]	gematik: Spezifikation der SMC-K, Version 1.2.0
[SSL]	Netscape: SSL3.0 Specification
[TID]	Spezifikation des Aufbaus der Telematik-ID für HBA und SMC, Version 1.0.0, 22.08.2008
[TR-03114]	BSI: TR-0311, Stapelsignatur mit dem Heilberufsausweis, Version 2.0, 19.10.2007, www.bsi.de/literat/tr/tr03114/BSI-TR-03114.pdf
[TR-03115]	BSI: TR-03115, Komfortsignatur mit dem Heilberufsausweis, Version 2.0, 19.10.2007, www.bsi.de/literat/tr/tr03115/BSI-TR-03115.pdf
[TR-03116]	BSI: TR-03116, Technische Richtlinie für die eCard-Projekte der Bundesregierung, Version 3.0, 08.04.2009, www.bsi.de/literat/tr/tr03116/BSI-TR-03116.pdf

3 Abkürzungen

3.1 Abkürzungen

AC	Attribute Certificate (Attributzertifikat)
AID	Application Identifier (Anwendungskennung)
AKS	Auslöser KomfortSignatur
AOD	Authentication Object Directory
APDU	Application Protocol Data Unit [ISO7816-3]
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)
CAMS	Card Application Management System
CAR	Certification Authority Reference
CC	Cryptographic Checksum (kryptographische Prüfsumme)
CD	Certificate Directory
CER	Canonical Encoding Rules
CG	Cryptogram
CH	Cardholder (Karteninhaber)
CHA	Certificate Holder Authorization
CHR	Certificate Holder Reference
CIA	Cryptographic Information Application
CIO	Cryptographic Information Objects
CLA	Class-Byte einer Kommando-APDU

COS	Card Operating System (Chipkartenbetriebssystem)
CPI	Certificate Profile Identifier
CRL	Certificate Revocation List (Zertifikatssperrliste)
CS	CertSign (CertificateSigning)
CTA	Card Terminal Application (Kartenterminalanwendung)
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
ECDSA	Elliptic Curve Digital Signature Algorithm
EF	Elementary File
eGK	elektronische Gesundheitskarte [eGK-P1] und [eGK-P2]
EHIC	European Health Insurance Card
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 Platform
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
KeyRef	Key Reference
KM	Komfortmerkmal
KT	Karten-Terminal
LCS	Life Cycle Status
LSB	Least Significant Byte(s)
MAC	Message Authentication Code
MF	Master File
MII	Major Industry Identifier
MSE	Manage Security Environment
OCSP	Online Certificate Status Protocol
OD	Object Directory
OID	Object Identifier
OSIG	Organisationssignatur
PIN	Personal Identification Number
PIX	Proprietary Application Provider Extension
PK,PuK	Public Key
PKCS	Public Key Cryptography Standard (hier[PKCS#1])
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure for X.509 Certificates (IETF)
PP	Protection Profile (Schutzprofil)
PrK	Private Key
PSO	Perform Security Operation
PUK	Personal Unblocking Key (Resetting Code)
PV	Plain Value
P1	Parameter P1 einer Kommando-APDU
P2	Parameter P2 einer Kommando-APDU
QES	Qualifizierte Elektronische Signatur
RA	Registration Authority (Registrierungsinstanz)
RAM	Random Access Memory
RC	Retry Counter (Fehlbedienungszähler)
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 [RSA]
SAK	Signaturanwendungskomponente
SE	Security Environment (Sicherheitsumgebung)
SFID	Short EF Identifier
SIG	Signatur
SigG	Signaturgesetz [SigG01]
SigV	Signaturverordnung [SigV01]
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 [SSL]
SUK	Stapel- und Komfortsignatur
TLV	Tag Length Value
TC	Trusted Channel
TLS	Transport Layer Security
UID	User Identification
UTF8	8-bit Unicode Transformation Format
WTLS	Wireless Transport Layer Security
ZDA	Zertifizierungsdiensteanbieter
3TDES	3-Key-Triple-DES

3.2 Notation

Für Schlüssel und Zertifikate wird die folgende vereinfachte Backus-Naur-Notation verwendet (zu den Festlegungen siehe [PKI-Nota]):

<object descriptor> ::= <key descriptor> | <certificate descriptor>

<key descriptor> ::= <key>.<keyholder>.<key usage>

<key> ::= <private key> | <public key> | <secret key>

<private key> ::= PrK (asym.)

<public key> ::= PuK (asym.)

<secret key> ::= SK (sym.)

<keyholder> ::= <health professional> | <card holder> | <certification authority> |
 <health professional card> | <card application management system> |
 <health care institution> | <security module card> | <signature application component> |
<security module card terminal> |
 <electronic health card>

<health professional> ::= HP

<card holder> ::= CH

<certification authority> ::= <root certification authority> |
 <certification authority for CAMS of HPC> | <certification authority for HPC> |
 <certification authority for SMC> | <certification authority for eGK> |
 <certification authority for comfort signature trigger>

<root certification authority> ::= RCA

<certification authority for card application management system of health professional card> ::=
 CA_CAMS_HPC

<certification authority for health professional card> ::= CA_HPC

<certification authority for security module card> ::= CA_SMC

<certification authority for electronic health card> ::=

 CA_eGK (CA elektronische Gesundheitskarte)

<certification authority for comfort signature trigger> ::= CA_KM (CA Komfortmerkmal)

<health professional card> ::= HPC

<card application management system> ::= CAMS

<health care institution> ::= HCI

<security module card> ::= SMC

<signature application component> ::= SAK

<security module card terminal> ::= SMKT

<electronic health card> ::= eGK (elektronische Gesundheitskarte)

<key usage> ::= <organizational signature> | <encipherment> | <authentication> |
 <certsign cvc> | <certsign x509>

<organizational signature> ::= OSIG

<encipherment> ::= ENC

<certsign cvc> ::= CS

<certsign x509> ::= CA

<authentication> ::= AUT | <cv based authentication>

<cv based authentication> ::= <role authentication> | <device authentication>

<role authentication> ::= AUTR_CVC

<device authentication> ::= AUTD_CVC | <remote pin sender> | <remote pin receiver> |
<stack and comfort signature card> | <comfort signature trigger> |
<signature application component>

<remote pin Sender>:: = AUTD_RPS_CVC (Remote PIN Sender)
<remote pin Receiver>::= AUTD_RPE_CVC (Remote PIN Empfänger)
<stack and comfort signature card>::= AUTD_SUK_CVC (Stapel- und Komfortsignatur)
<comfort signature trigger>::= AUTD_AKS_CVC (Auslöser Komfort Signatur)

<certificate descriptor>::=
<certificate>.<certificate holder>.<certificate usage>

<certificate>::= C

<certificate holder>::=
<health professional> | <certification authority> | <health professional card> |
<card application management system> | <security module card> |
<security module card terminal> | <electronic health card>

<certificate usage>::=
<organizational signature> | <encipherment> | <authentication> | <certsign cvc> |
<certsign x509>

Für eine Sequenz von Datenelementen wird die folgende Notation verwendet:

|| = Konkatenation von Daten

Zur Vereinfachung werden X.509v3-Zertifikate ohne Versionsnummer bezeichnet.

4 Typen von Sicherheitsmodulkarten

Eine SMC bietet vergleichbare Funktionen wie eine HPC, aber die X.509-Zertifikate - falls sie vorhanden sind – beziehen sich nicht auf eine Person, sondern auf eine organisatorische Instanz des Gesundheitswesens (z.B. Praxis, Apotheke, Krankenhaus oder Abteilung).

Folgende SMC-Typen müssen unterschieden werden:

Tabelle 1 – (N3001.00) SMC-Typen

SMC-Typ	Funktionalität	Anwendungsfälle
SMC-A z.B. genutzt in Kartenterminals ("Arbeitsplatzkarte")	Asymmetrisches CVC-Authentisierungsverfahren ohne Aufbau eines Trusted Channel	SMC-A Autorisierung, Zugriff auf eGK nach Autorisierung der SMC-A
	Asymmetrisches CVC-Authentisierungsverfahren mit Aufbau eines Trusted Channel	SMC-A als PIN-Sender: Gesicherte PIN-Übertragung an eine HPC, eine SMC-B oder einen RFID-Token
	Unterstützung eines Trusted Channel, d.h. PSO-Operationen COMPUTE CC, ENCIPHER, DECIPHER, VERIFY CC, und (optional) ENVELOPE Kommando für die Verarbeitung von SM-Datenobjekten	SMC-A als PIN-Sender: Gesicherte PIN-Übertragung an eine HPC, eine SMC-B oder einen RFID-Token
	Persistente Speicherung von Sitzungsschlüsseln (Vorstellungsschlüssel) für eine performantere symmetrische C2C-Authentisierung	SMC-A als PIN-Sender: Gesicherte PIN-Übertragung an eine HPC, eine SMC-B oder einen RFID-Token
	Symmetrisches CVC-Authentisierungsverfahren mit Aufbau eines Trusted Channel	SMC-A als PIN-Sender: Gesicherte PIN-Übertragung an eine HPC, eine SMC-B oder einen RFID-Token
	KT-Anwendung (DF.KT) zur Authentisierung des Kartenterminals	Authentisierung des Kartenterminals gegenüber dem Konnektor unter Nutzung des Authentisierungsschlüssels in der SMC-A
SMC-B z.B. einmal pro Organisationseinheit genutzt in Kartenterminal ("Institutionenkarte")	Funktionalität der SMC-A	Anwendungsfälle der SMC-A
	PIN.SMC für die HP-Authentisierung	SMC-B Autorisierung
	Unterstützung von Secure Messaging, d.h. Verarbeitung von SM-Kommandos	SMC-B als PIN-Empfänger: Sicherer Empfang von PIN.SMC
	PKI-Schlüssel für OSIG, ENC & AUT und zugehörige X.509-Zertifikate (keine Attributzertifikate)	PKI - Services für die zugehörige Institution: - Entschlüsselung von verschlüsselten Dokumenten, die an die entsprechende Institution und nicht an eine Person adressiert sind - Client/Server Authentifizierung - Erzeugung von Organisationssignaturen
	EF.CONF für Konfigurationsdaten des Konnektors	Bereitstellung von Konfigurationsdaten für die Konnektorwartung (hoher Sicherheitslevel)
EF.NET für Konfigurationsdaten des Netzwerks	Bereitstellung von Konfigurationsdaten für das Netzwerk (niedrigerer Sicherheitslevel)	

5 Sicherheitsmodulkarte A

5.1 ATR-Kodierung und technische Eigenschaften

Für die SMC-A gelten dieselben Konventionen für die technischen Eigenschaften, ATR und Übertragungsprotokolle wie für die HPC, siehe [HPC-P1]. Siehe Kapitel 11.2 in [HPC-P1] für die elektrische Schnittstelle und Kapitel 4.1 in [HPC-P2] für die ATR-Kodierung. Die SMC-A ist als Plug-In-Karte (ID-000) für die Nutzung in entsprechenden Kartenterminals vorgesehen.

5.2 Allgemeine Struktur

Die SMC-A enthält

- die Root-Anwendung (MF) mit einigen EFs auf MF-Ebene für allgemeine Datenobjekte, CV-Zertifikate und globale Schlüssel für Authentisierungsprozesse (z.B. Nachweis der Zugriffsberechtigung auf die eGK und Prüfen der Echtheit der eGK),
- die Sicherheitsmodulanwendung (DF.SMA) zur Bereitstellung von SMC-A-spezifischen Dateien
- die Kartenterminalanwendung (DF.KT) für die Authentisierung des Kartenterminals zum Verbindungsaufbau mit einem Konnektor.

Abbildung 1 (N3002.00) zeigt die prinzipielle Struktur der SMC-A.

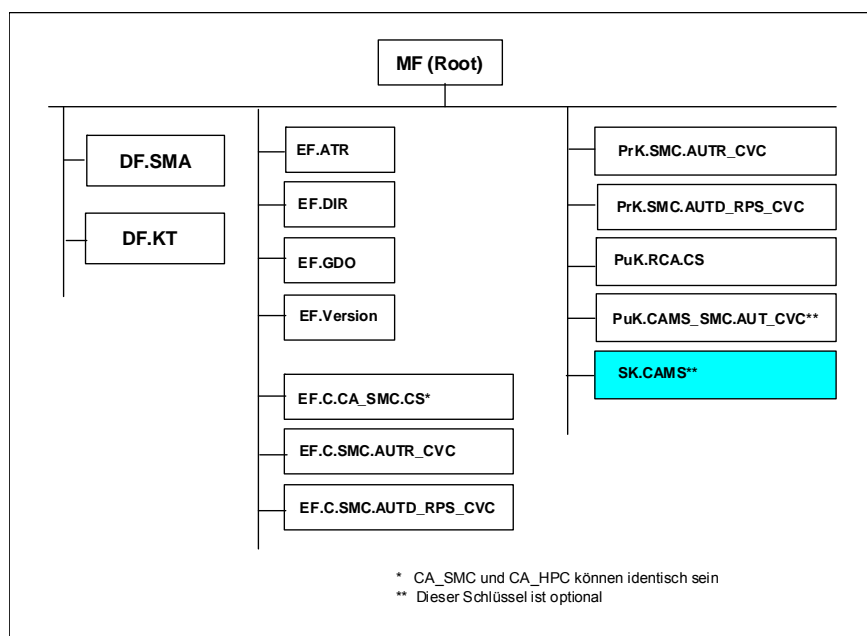


Abbildung 1 – (N3002.00) Allgemeine Dateistruktur der SMC-A

5.3 Root-Anwendung und Dateien auf MF-Ebene

5.3.1 MF

Das MF der SMC-A ist ein "Application Dedicated File" (siehe Kapitel 8.3.1.3 in [HPC-P1]) mit den in Tabelle 2 (N3003.00) aufgeführten Eigenschaften.

Tabelle 2 – (N3003.00) Attribute von MF

Attribut	Wert	Anmerkung
Objekttyp	Application Dedicated File	
Application Identifier	'D27600014604'	
File Identifier	'3F00'	Optional vorhanden
Life Cycle Status	Operational State (activated)	
Zugriffsregel in allen SEs		
Zugriffsart	Sicherheitsbedingung	Anmerkung
SELECT	ALWAYS	
LOAD APPLICATION (nach Ausgabe der SMC-A)	AUT('D27600014600' '01') AND SmMac AND SmCmdEnc	Nur ausführbar, wenn ein CAMS genutzt wird, siehe Kapitel 5.12. Falls ein CAMS mit symmetrischer Authentisierung eingesetzt wird, muss die Sicherheitsbedingung die Schlüsselreferenz des entsprechenden symmetrischen Schlüssels enthalten, d.h. AUT('13') statt AUT('D27600014600' '01')
ACTIVATE, DEACTIVATE, DELETE	NEVER	

5.3.2 EF.ATR

Die transparente Datei EF.ATR enthält ein zusammengesetztes Datenobjekt zur Anzeige der I/O-Puffer-Größen und das DO 'Pre-issuing Data', das für die CAMS-Dienste von Bedeutung ist. Die folgende Tabelle zeigt die Eigenschaften von EF.ATR.

Tabelle 3 – (N3004.00) Attribute von MF / EF.ATR

Attribut	Wert	Anmerkung
Objekttyp	Transparent Elementary File	
File Identifier	'2F01'	Gemäß [ISO7816-4]
Short File Identifier	'1D' = 29	
Number of Bytes	COS-spezifisch	
Flag Transaction Mode	False	
Flag Checksum	True	
Life Cycle Status	Operational State (activated)	
Content	...	siehe Tabelle 4 (N3005.00)
Zugriffsregel in allen SEs		
Zugriffsart	Sicherheitsbedingung	Anmerkung
SELECT, READ BINARY	ALWAYS	
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, UPDATE BINARY	NEVER	

Der Inhalt von EF-ATR ist in den folgenden Tabellen spezifiziert.

Tabelle 4 – (N3005.00) Inhalt von EF.ATR

Tag	L	Wert	Bedeutung
'E0'	'xx'	'02 xx xxxx 02 xx xxxx 02 xx xxxx 02 xx xxxx'	DO I/O-Puffergrößen, siehe Tabelle 5 (N3006.00)
'66'	'xx'	'46 xx ...' siehe Tabelle 6 (N3007.00) '47 04 x6 21 Dx xx', siehe Tabelle 7 (N3008.00) und Tabelle 8 (N3009.00)	DO Card Data: DO Pre-issuing data DO Card Capabilities mit 4. Byte = Unterstützte Trusted Channel-Verfahren

Das Datenobjekt I/O-Puffergrößen hat, wie in Tabelle 5 (N3006.00) gezeigt, 4 eingebettete Datenobjekte (Tag '02' = Integer-Wert, Längenfeld 1 Byte mit Wert '02' oder '03', Wertefeld = maximale Anzahl von Bytes der entsprechenden APDU).

Tabelle 5 – (N3006.00) Datenobjekt Input/Output-Puffergrößen

Tag	Länge	Wert
'E0'	'xx'	'02' -L-'xxxx' '02' -L-'xxxx' '02'-L-'xxxx' '02'-L-'xxxx' = - DO max. Länge der Kommando-APDU ohne SM - DO max. Länge der Antwort-APDU ohne SM - DO max. Länge der Kommando-APDU mit SM - DO max. Länge der Antwort-APDU mit SM

Anmerkung – Im Gegensatz zum Hinweis 1 in Kapitel 11.5.5 von [HPC-P1] und Hinweis 1 in Kapitel 11.5.6 von [HPC-P1] ist es nicht möglich, maximale Längen in Abhängigkeit von bestimmten Kombinationen CLA, INS, P1 und P2 auszudrücken. Das wird möglicherweise in späteren Versionen dieses Dokuments definiert, sobald geeignete Datenstrukturen in [ISO7816-4] aufgenommen sind.

Tabelle 6 – (N3007.00) Wert des DO Pre-issuing data (Tag '46')

L (Bytes)	Bedeutung der konkatenierten Datenelemente (höchstwertiges Byte: ICM)
1	IC-Herstellererkennung (siehe www.sc17.com)
5	Kartenherstellererkennung (siehe DIN-RA: http://sit.sit.fraunhofer.de/karten_ident/SIT/rid_sde)
x	IC-ID (Kartenhersteller-spezifisch)
x	COS-Version (Kartenhersteller-spezifisch)
x	ROM-Maske (Kartenhersteller-spezifisch)

Tabelle 7 – (N3008.00) Wert of DO Card Capabilities (Tag '47')

b8	b7	b6	b5	b4	b3	b2	b1	Bedeutung des 1. Byte ('x6')
1	-	-	-	-	-	-	-	DF-Auswahl mit vollem DF-Namen
-	x	-	-	-	-	-	-	DF-Auswahl mit partiellem DF-Namen (nicht festgelegt)
-	-	x	-	-	-	-	-	DF- Auswahl mit Pfad (nicht festgelegt)
-	-	-	1	-	-	-	-	DF- Auswahl mit File Identifier
-	-	-	-	0	-	-	-	Implizite DF-Auswahl (nicht unterstützt)
-	-	-	-	-	1	-	-	Unterstützung der Short File Identifier
-	-	-	-	-	-	1	-	Unterstützung von Recordnummern
-	-	-	-	-	-	-	0	Record Identifier (nicht unterstützt)
b8	b7	b6	b5	b4	b3	b2	b1	Bedeutung de 2. Byte ('21')
0	-	-	-	-	-	-	-	EFs mit TLV-Struktur (nicht unterstützt)
-	0	1	-	-	-	-	-	Verhalten der Schreibfunktionen (proprietär)
-	-	-	0	-	-	-	-	Wert 'FF' als 1. Byte von BER-TLV Tagfeldern unzulässig
-	-	-	-	0	0	0	1	Größe der Dateneinheiten in Vierbit-Einheiten (als Zweierpotenz, d.h. '01' = 2 Vierbit-Einheiten = 1 Byte)
b8	b7	b6	b5	b4	b3	b2	b1	Bedeutung des 3. Byte ('Dx')
1	-	-	-	-	-	-	-	Unterstützung von Command Chaining, siehe Anmerkung 1
-	1	-	-	-	-	-	-	Extended Lc und Le-Felder
-	-	0	-	-	-	-	-	b6 ist RFU (b6 = 0 empfohlen)
-	-	-	1	0	-	-	-	Zuweisung der Nummern logischer Kanäle durch die Karte
-	-	-	-	-	y	z	t	
-	-	-	-	-	x	x	x	Maximale Anzahl logischer Kanäle, siehe Anmerkung 2

Anmerkung 1 – Command Chaining wird evt. für das Kommando LOAD APPLICATION gebraucht, siehe Kapitel 5.12.

Anmerkung 2 – Die Card-Capability-Bytes sind gemäß Kapitel 8.1.1.2.7 in [ISO7816-4] gestaltet. Im 3. Byte kodieren die Bits b3-b1 die maximale Anzahl logischer Kanäle, die von der Karte unterstützt wird: Wenn y, z, t nicht durchgehend auf 1 gesetzt sind, werden $4y+2z+t+1$ logische Kanäle unterstützt, d.h. eins bis sieben. $y = z = t = 1$ bedeutet Unterstützung von acht oder mehr logischen Kanälen. Die maximale Anzahl logischer Kanäle muss auf einen der folgenden Werte gesetzt sein: b3b2b1 = 011 (4 Kanäle), 100 (5 Kanäle), 101 (6 Kanäle), 110 (7 Kanäle) oder 111 (≥ 8 Kanäle).

Tabelle 8 – (N3009.00) Wert des 4. Card Capabilities Byte: Unterstützte Trusted Channel Verfahren

b8	b7	b6	b5	b4	b3	b2	b1	Bedeutung
x	x	x	x	x	x	0	0	Keine Information
						0	1	PSO
						1	1	PSO und ENVELOPE

5.3.3 EF.DIR

EF.DIR enthält die Anwendungs-Templates für MF, DF.SMA und DF.KT gemäß ISO/IEC 7816-4. EF.DIR erlaubt das Hinzufügen von Anwendungskennungen weiterer (nachgeladener) Anwendungen, siehe Eigenschaften von EF.DIR in der folgenden Tabelle.

Tabelle 9 – (N3010.00) Attribute von MF / EF.DIR

Attribut	Wert	Anmerkung
Objekttyp	Linear Variable Record Elementary File	
File Identifier	'2F00'	
Short File Identifier	'1E = 30	
Number of Bytes	114	6 * 19 Bytes
Maximum Number of Records	6 (3 für zukünftige Verwendung)	
Maximum Record Length	19 Bytes	
Flag Record LCS	False	
Flag Transaction Mode	True	
Flag Checksum	True	
Life Cycle Status	Operational State (activated)	
Content	...	siehe Tabelle 10 (N3011.00)
Zugriffsregel in allen SEs		
Zugriffsart	Sicherheitsbedingung	Anmerkung
SELECT, READ RECORD, SEARCH RECORD	ALWAYS	
APPEND RECORD, UPDATE RECORD	AUT('D27600014600' '01') AND SmMac	Nur ausführbar, wenn ein CAMS genutzt wird, siehe Kapitel 5.12. Falls ein CAMS mit symmetrischer Authentisierung eingesetzt wird, muss die Sicherheitsbedingung die Schlüsselreferenz des entsprechenden symmetrischen Schlüssels enthalten, d.h. AUT('13') statt AUT('D27600014600' '01')
ACTIVATE, ACTIVATE RECORD, DEACTIVATE, DEACTIVATE RECORD, DELETE, ERASE RECORD	NEVER	

Tabelle 10 (N3011.00) zeigt die in EF.DIR enthaltenen Anwendung-Templates.

Tabelle 10 – (N3011.00) Anwendungs-Templates in EF.DIR einer SMC-A

Tag	L	Anwendungs-Template	Bedeutung
'61'	'08'	'4F 06 D27600014604'	Anwendungs-Template mit AID.MF
'61'	'08'	'4F 06 D27600014605'	Anwendungs-Template mit AID.SMA
'61'	'08'	'4F 06 D27600014400'	Anwendungs-Template mit AID.KT

5.3.4 EF.GDO

Tabelle 11 (N3012.00) zeigt die Eigenschaften von EF.GDO.

Tabelle 11 – (N3012.00) Attribute von MF / EF.GDO

Attribut	Wert	Anmerkung
Objektyp	Transparent Elementary File	
File Identifier	'2F02'	
Short File Identifier	'02' = 2	
Number of Bytes	12	
Flag Transaction Mode	False	
Flag Checksum	True	
Life Cycle Status	Operational State (activated)	
Content	...	siehe Tabelle 12 (N3013.00)
Zugriffsregel in allen SEs		
Zugriffsart	Sicherheitsbedingung	Anmerkung
SELECT, READ BINARY	ALWAYS	
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, UPDATE BINARY	NEVER	

EF.GDO beinhaltet in Übereinstimmung mit [Resolution190] das Datenobjekt ICC-Seriennummer Tabelle 12 (N3013.00).

Tabelle 12 – (N3013.00) Datenobjekt ICCSN in EF.GDO

Tag	L	Wert	Bedeutung
'5A'	'0A'	'80276 ...'	ICCSN

Abbildung 2 (N3014.00) zeigt den Aufbau des Datenobjekts ICCSN (Tag '5A') für Karten im Gesundheitswesen.

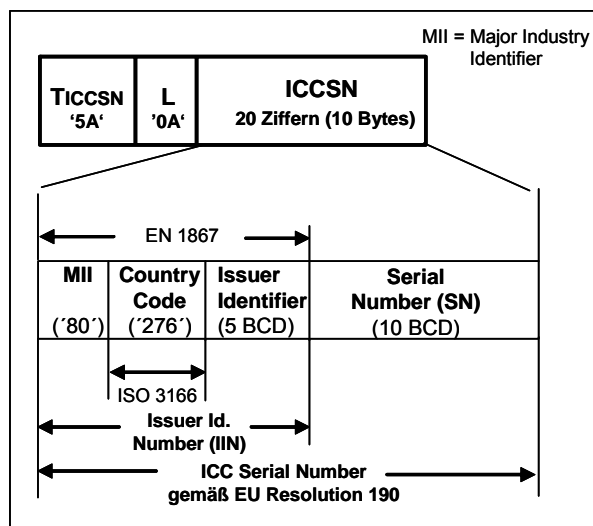


Abbildung 2 - (N3014.00) ICCSN für Karten im Gesundheitswesen

Nur registrierte IINs sind als Teil der ICCSN zugelassen, siehe Annex A.1 in [HPC-P2].

Der Kartenherausgeber muss sicherstellen, dass die Seriennummer (SN) eineindeutig ist (insbesondere, wenn verschiedene Kartenhersteller beteiligt sind). Die zwei führenden BCDs der Seriennummer (im Anschluss an die Kennung des Herausgebers) geben den beteiligten Zertifizierungsdiensteanbieter an, siehe Annex A.2 in [HPC-P2].

5.3.5 EF.Version

EF.Version enthält Records fester Länge mit den Versionsnummern der Spezifikationsteile und eine SRQ-Nummer (welche die Obergrenze der relevanten SRQs anzeigt), auf denen die Karte beruht. Die nachfolgende Tabelle zeigt die Eigenschaften von EF.Version.

Tabelle 13 – (N3015.00) Attribute von MF / EF.Version

Attribut	Wert	Anmerkung
Objektyp	Linear Fix Record Elementary File	
File Identifier	'2F10'	
Short File Identifier	'10' = 16	
Number of Bytes	20	
Maximum Number of Records	4	
Maximum Record Length	5 Bytes	
Flag Record LCS	False	
Flag Transaction Mode	True	
Flag Checksum	True	
Life Cycle Status	Operational State (activated)	
Content	...	siehe Tabelle 14 (N3016.00).
Zugriffsregel in allen SEs		
Zugriffsart	Sicherheitsbedingung	Anmerkung
SELECT, READ RECORD, SEARCH RECORD	ALWAYS	
UPDATE RECORD	AUT('D27600014600' '01') AND SmMac	Nur ausführbar, wenn ein CAMS genutzt wird, siehe Kapitel 5.12. Falls ein CAMS mit symmetrischer Authentisierung eingesetzt wird, muss die Sicherheitsbedingung die Schlüsselreferenz des entsprechenden symmetrischen Schlüssels enthalten, d.h. AUT('13') statt AUT('D27600014600' '01').
ACTIVATE, ACTIVATE RECORD, APPEND	NEVER	

RECORD, DEACTIVATE, DEACTIVATE RECORD, DELETE, ERASE RECORD		
---	--	--

Die Datei EF.Version enthält 4 Records fester Länge, siehe Tabelle 14 (N3016.00). Die ersten 3 Records zeigen die 3 Teile der HPC-Spezifikation und eine SRQ-Nummer an, die zur Karte in Beziehung stehen. Das Tripel Versionsnummer XX.YY.ZZ des entsprechenden Spezifikationsteils ist zusammen mit der vierstelligen SRQ-Nummer SSSS als XXYYZZSSSS in BCDs kodiert. Der letzte Record ist für eine zukünftige Nutzung reserviert (RFU).

Tabelle 14 – (N3016.00) Inhalt von EF.Version

Recordnr.	Wert (5 Bytes)	Bedeutung
1	'0203020000'	Version der unterstützten HPC-Spezifikation Teil 1, gefolgt von der Obergrenze der SRQ-Nummern, mit der die Karte konform ist Hier: Version 2.3.2, keine weiteren SRQs
2	'0203020000'	Version der unterstützten HPC-Spezifikation Teil 2, gefolgt von der Obergrenze der SRQ-Nummern, mit der die Karte konform ist Hier: Version 2.3.2, keine weiteren SRQs
3	'0203020000'	Version der unterstützten HPC-Spezifikation Teil 3, gefolgt von der Obergrenze der SRQ-Nummern, mit der die Karte konform ist Hier: Version 2.3.2, keine weiteren SRQs
4	'0000000000'	RFU

5.3.6 EF.C.CA_SMC.CS

EF.C.CA_SMC.CS enthält das CV-Zertifikat des Zertifizierungsdiensteanbieters, das von der Wurzel-CA für das Gesundheitswesen für eine CA_SMC ausgegeben wurde. Alle CV-Zertifikate einer HPC oder SMC stammen von derselben Wurzel-Zertifizierungsinstanz für CV-Zertifikate. Tabelle 15 (N3017.00) zeigt die Eigenschaften der Datei EF.C.CA_SMC.CS.

Tabelle 15 – (N3017.00) Attribute von MF / EF.C.CA_SMC.CS

Attribut	Wert	Anmerkung
Objekttyp	Transparent Elementary File	
File Identifier	'2F04'	
Short File Identifier	'04' = 4	
Number of Bytes	331	
Flag Transaction Mode	False	
Flag Checksum	False	
Life Cycle Status	Operational State (activated)	
Content	...	siehe [HPC-P2], Tabelle (N2019.00)
Zugriffsregel in allen SEs		
Zugriffsart	Sicherheitsbedingung	Anmerkung
SELECT, READ BINARY	ALWAYS	
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, UPDATE BINARY	NEVER	

Die Kodierung von CV-Zertifikaten für ZDAs und die enthaltene OID sind in Kapitel 4.3.6 von [HPC-P2] beschrieben. Struktur und Inhalt des CVCs in EF.C.CA_SMC.CS mit CPI = '21' sind in Kapitel 7.1 von [HPC-P1] definiert und in [Tabelle \(N2019.00\)](#) von [HPC-P2] dargestellt.

5.3.7 EF.C.SMC.AUTR_CVC

EF.C.SMC.AUTR_CVC enthält das CV-Zertifikat der SMC-A für die rollenbasierte C2C-Authentisierung zwischen eGK/SMC und die Autorisierungsprozesse zwischen HPC/SMC bzw. SMC/SMC. Die folgende Tabelle zeigt die Eigenschaften der Datei.

Tabelle 16 – (N3018.00) Attribute von MF / EF.C.SMC.AUTR_CVC

Attribut	Wert	Anmerkung
Objekttyp	Transparent Elementary File	
File Identifier	'2F03'	
Short File Identifier	'03' = 3	
Number of Bytes	341	
Flag Transaction Mode	False	
Flag Checksum	False	
Life Cycle Status	Operational State (activated)	
Content	...	siehe [HPC-P2], Tabelle (N2021.00)
Zugriffsregel in allen SEs		
Zugriffsart	Sicherheitsbedingung	Anmerkung
SELECT, READ BINARY	ALWAYS	
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, UPDATE BINARY	NEVER	

Die Kodierung des CV-Zertifikats der SMC-A und die enthaltene OID sind in [Kapitel 4.3.6](#) und [Kapitel 4.3.7](#) von [HPC-P2] beschrieben. Struktur und Inhalt des CVC in EF.C.SMC.AUTR_CVC mit CPI = '22' sind in Kapitel 7.1 von [HPC-P1] spezifiziert und in [Tabelle \(N2021.00\)](#) von [HPC-P2] dargestellt.

Die „Certificate Holder Authorizations“ für C.SMC.AUTR_CVC und für andere CV-Zertifikate der Karten im Gesundheitswesen sind in [Tabelle \(N2623.00\)](#) des Annex A.3 von [HPC-P2], dargestellt.

5.3.8 EF.C.SMC.AUTD_RPS_CVC

EF.C.SMC.AUTD_RPS_CVC enthält das CV-Zertifikat einer SMC-A für funktionsbasierte C2C-Authentisierungsprozesse zur Übertragung einer eingegebenen PIN an eine HPC, eine SMC-B oder einen RFID-Token, siehe Anmerkung. Dieses Zertifikat kann ohne PIN-Authentisierung genutzt werden.

ANMERKUNG – Sowohl die Präsentation des RFID-Token, als auch die PIN-Eingabe für einen RFID-Token erfolgt lokal voraussichtlich an demselben Authentisierungsterminal, nutzt aber den Modus für entfernte PIN-Übertragung, um die Daten an der Luftschnittstelle abzusichern.

Tabelle 17 – (N3019.00) Attribute von MF / EF.C.SMC.AUTD_RPS_CVC

Attribut	Wert	Anmerkung
Objekttyp	Transparent Elementary File	
File Identifier	'2F06'	
Short File Identifier	'06' = 6	
Number of Bytes	341	
Flag Transaction Mode	False	
Flag Checksum	False	
Life Cycle Status	Operational State (activated)	
Content	...	siehe [HPC-P2], Tabelle (N2021.00)
Zugriffsregel in allen SEs		
Zugriffsart	Sicherheitsbedingung	Anmerkung
SELECT, READ BINARY	ALWAYS	

ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, UPDATE BINARY	NEVER	
---	-------	--

Die Kodierung des CV-Zertifikats der SMC-A und die enthaltene OID sind in [Kapitel 4.3.6](#) und [Kapitel 4.3.7](#) von [HPC-P2] beschrieben. Struktur und Inhalt des CVC in EF.C.SMC.AUTD_RPS_CVC mit CPI = '22' sind in Kapitel 7.1 von [HPC-P1] definiert und in [Tabelle \(N2021.00\)](#) von [HPC-P2] dargestellt.

Die "Certificate Holder Authorization" für C.SMC.AUTD_RPS_CVC ist in [Tabelle \(N2624.00\)](#) des Annex A.3 von [HPC-P2] beschrieben.

5.3.9 PrK.SMC.AUTR_CVC

PrK.SMC.AUTR_CVC ist der globale private Schlüssel für die C2C-Authentisierung zwischen SMC/eGK. Die Nutzung des privaten Schlüssels muss durch einen Heilberufler mit einem zugehörigen Profil autorisiert werden, d.h. durch externe Authentisierung einer HPC oder einer SMC (siehe Kapitel 5.7) mit passender Rollenennung der über die Karte verfügbenden Person/Institution, siehe [Tabelle \(N2623.00\)](#) in Annex A.3 von [HPC-P2]. Die Eigenschaften des Schlüssels sind in Tabelle 18 (N3020.00) dargestellt.

Tabelle 18 – (N3020.00) Attribute von MF / PrK.SMC.AUTR_CVC

Attribut	Wert	Anmerkung
Objekttyp	Privates RSA-Objekt	Profil 2 oder 3 oder ...
Key Identifier	'10'	
Key Reference	'10'	
Private Key	... (2048 Bits)	Wird personalisiert
Algorithm Identifier	rsaRoleAuthentication rsaSessionkey4SM rsaSessionkey4TC	
Zugriffsregel in allen SEs		
Zugriffsart	Sicherheitsbedingung	Anmerkung
INTERNAL AUTHENTICATE	AUT('D27600004000' 'xx')	Rollenauthentisierung einer HPC oder SMC mit zugehörigem persönlichen Profil, z.B. Profil 2, siehe [HPC-P2], Tabelle (N2623.00) .
EXTERNAL AUTHENTICATE	ALWAYS	
Andere	NEVER	

Der öffentlichen Schlüssel zu PrK.SMC.AUTR_CVC (eines CVC-Inhabers mit Profil 2 oder 3 oder...) ist in der Datei C.SMC.AUTR_CVC enthalten.

5.3.10 PrK.SMC.AUTD_RPS_CVC

PrK.SMC.AUTD_RPS_CVC ist der globale private Schlüssel für C2C-Authentisierung zwischen SMC/HPC, SMC/SMC oder SMC/RFID-Token für die PIN-Übertragung zur PIN-empfangenden Karte (HPC, SMC-B, RFID-Token). Die Nutzung des privaten Schlüssels erfordert die externe Authentisierung einer Karte mit der Funktionalität des PIN-Empfängers (Profil 53 der HPC bzw. Profil 55 der SMC-B oder des RFID-Token, siehe [Tabelle \(N2624.00\)](#) in Annex A.3 von [HPC-P2]). Die Eigenschaften des Schlüssels sind in Tabelle 19 (N3021.00) dargestellt.

Tabelle 19 – (N3021.00) Attribute von MF / PrK.SMC.AUTD_RPS_CVC

Attribut	Wert	Anmerkung
Objekttyp	Privates RSA-Objekt	Profil 54 (PIN Sender)
Key Identifier	'12'	
Key Reference	'12'	
Private Key	... (2048 Bits)	Wird personalisiert
Algorithm Identifier	rsaSessionkey4TC rsaSessionkey4Intro	
Zugriffsregel in allen SEs		
Zugriffsart	Sicherheitsbedingung	Anmerkung
INTERNAL AUTHENTICATE	AUT('D27600004000' '35') OR AUT('D27600004000' '37')	Funktionale Geräteauthentisierung einer HPC (SSCD mit Profil 53), einer SMC oder eines RFID-Token (PIN-Empfänger mit Profil 55), siehe [HPC-P2], Tabelle (N2624.00)
EXTERNAL AUTHENTICATE	ALWAYS	
Andere	NEVER	

Die öffentliche Schlüssel PrK.SMC.AUTD_RPS_CVC (eines CVC-Inhabers mit Profil 54) ist in der Datei C.SMC.AUTD_RPS_CVC enthalten.

5.3.11 PuK.RCA.CS

PuK.RCA.CS ist der öffentliche Schlüssel der Wurzel-CA für die Prüfung der von dieser Zertifizierungsinstanz ausgegebenen CVCs. Die folgende Tabelle zeigt die Eigenschaften des öffentlichen Schlüssels.

Tabelle 20 – (N3022.00) Attribute von MF / PuK.RCA.CS

Attribut	Wert	Anmerkung
Objekttyp	Öffentliches RSA-Signaturprüfungsobjekt	
Key Identifier	CAR of C.CA_SMC.CS : ZDA-Kennung (5 Bytes) Erweiterung (3 Bytes)	Wird personalisiert
Key Reference	-	
Public Key	... (2048 Bits)	Wird personalisiert
OID	'2B240304020204' = {1 3 36 3 4 2 2 4}	
Zugriffsregel in allen SEs		
Zugriffsart	Sicherheitsbedingung	Anmerkung
VERIFY CERTIFICATE	ALWAYS	
Andere	NEVER	

5.3.12 PuK.CAMS_SMC.AUT_CVC

PuK.CAMS_SMC.AUT_CVC (optional) ist der öffentliche Schlüssel zur Durchführung des SMC/CAMS-Authentisierungsverfahrens mit Aufbau eines Trusted Channel. Die folgende Tabelle zeigt die Eigenschaften des öffentlichen Schlüssels.

Tabelle 21 – (N3023.00) Attribute von MF / PuK.CAMS_SMC.AUT_CVC

Attribut	Wert	Anmerkung
Objekttyp	Öffentliches RSA-Authentisierungsobjekt	
Key Identifier	'0000000000000000000000000000000013' (12 byte)	Wird personalisiert
CHA	'D2760001460001'	
Public Key	... (2048 Bits)	Wird personalisiert
OID	'2B2403050204' = {1 3 36 3 5 2 4}	
Algorithm Identifier	rsaSessionkey4SM	

Zugriffsregel in allen SEs		
Zugriffsart	Sicherheitsbedingung	Anmerkung
INTERNAL AUTHENTICATE	ALWAYS	
EXTERNAL AUTHENTICATE	ALWAYS	
Andere	NEVER	

5.3.13 SK.CAMS

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

Tabelle 22 – (N3024.00) Eigenschaften von MF / SK.CAMS

Attribut	Wert	Anmerkung
Object type	3TDES Authentication Object	
Key Identifier	'13' = 19	
encKey	...	Wird personalisiert
macKey	...	Wird personalisiert
Algorithm Identifier	desSessionkey4SM	
Zugriffsregeln in allen SEs		
Zugriffsart	Sicherheitsbedingung	Anmerkung
MUTUAL AUTHENTICATE	AUT('D27600004000' 'xx')	Rollenauthentisierung einer HPC oder SMC mit zugehörigem persönlichen Profil, z.B. Profil 2; siehe [HPC-P2], Tabelle (N2623.00).
Other	NEVER	

5.4 Sicherheitsumgebungen auf MF-Ebene

Auf MF-Ebene wird ausschließlich die Sicherheitsumgebung SE # 1 (Default-SE) verwendet. Es ist möglich, in SE # 1 einen Trusted Channel aufzubauen, um z.B. eine entfernte PIN-Eingabe an eine HPC, eine SMC-B oder einen RFID-Token durchzuführen oder Daten in zukünftigen Anwendungen online zu verarbeiten.

5.5 Öffnen der SMC-A

5.5.1 Auswahl der Root-Anwendung

Nach dem Reset ist die Root-Anwendung automatisch ausgewählt. Zu einem späteren Zeitpunkt kann die Root-Anwendung beispielsweise durch ein SELECT Kommando mit Anwendungskennung selektiert werden, wie in Tabelle 23 (N3025.00) gezeigt ist.

Tabelle 23 - (N3025.00) SELECT Kommando für MF-Auswahl

CLA	Gemäß ISO/IEC 7816-4
INS	'A4' = SELECT
P1	'04' = DF-Auswahl mittels AID
P2	'0C' = Keine FCI in der Antwort
Lc	'06' = Länge der AID im Datenfeld
Datenfeld	'D27600014604' = AID der Root-Anwendung (MF) der SMC-A
Le	Nicht vorhanden

Tabelle 24 - (N3026.00) SELECT Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	'9000' oder spezifische Status-Bytes, siehe [HPC-P1]

Anmerkung 1 – Der optionale FID '3F00' wird nicht für die MF-Auswahl verwendet, da nur im aktuellen Verzeichnis nach dem angegebenen FID gesucht wird, siehe Kapitel 14.2.6.10 von [HPC-P1].

5.5.2 Lesen von EF.ATR und EF.GDO

Zum Lesen von EF.ATR und EF.GDO wird das READ BINARY Kommando verwendet, siehe Kapitel 4.5.3 in [HPC-P2]. Da die SMC-A im jeweiligen Kartenleser verbleibt, braucht dieses Kommando wahrscheinlich jeweils nur einmal ausgeführt zu werden.

5.5.3 Lesen von EF.DIR und EF.Version

Zum Lesen von EF.DIR und EF.Version wird das READ RECORD Kommando verwendet, siehe Kapitel 4.5.4 in [HPC-P2]. Da die SMC-A im jeweiligen Kartenleser verbleibt, braucht dieses Kommando wahrscheinlich jeweils nur einmal ausgeführt zu werden.

5.5.4 Lesen der zur SMC-A gehörenden CV Zertifikate

Zum Lesen der zu einer SMC-A gehörenden CV-Zertifikate wird das READ BINARY Kommando verwendet, siehe Kapitel 4.5.5 in [HPC-P2]. Da die SMC-A im jeweiligen Kartenleser verbleibt, wird dieses Kommando wahrscheinlich jeweils nur einmal von der Softwareumgebung ausgeführt, in der die CV-Zertifikate z.B. zusammen mit der entsprechenden CHR der SMC-A gespeichert werden.

5.6 Management von Kanälen

Die SMC-A muss mindestens 4 logische Kanäle unterstützen, siehe Kapitel 11.4 in [HPC-P1]. Die maximale Anzahl logischer Kanäle wird in der Datei EF.ATR angezeigt, siehe Kapitel 5.3.2. Jeder Kanal besitzt seinen eigenen unabhängigen Sicherheitsstatus, d.h. eine externe Authentisierung der Rollenennung in einem logischen Kanal setzt keinen Sicherheitszustand in irgendeinem anderen Kanal.

Die Verwaltung der logischen Kanäle erfolgt wie in Kapitel 5 von [HPC-P2] beschrieben.

5.7 Autorisierung der SMC-A

Die allgemeinen Aspekte des Autorisierungsprozesses beschreibt Kapitel 7.6 in [HPC-P2] aus Sicht der autorisierenden Karte. Die Autorisierung der SMC-A wird technisch auf die Zugriffsregel des privaten Schlüssels PrK.SMC.AUTR_CVC (siehe Tabelle 18 (N3020.00)) abgebildet, der in C2C-Authentisierungsprozessen zum Einsatz kommt. Dieses Kapitel beschreibt die Kommandos, welche auf Seiten der zu autorisierenden SMC-A erforderlich sind.

Die Autorisierung wird durch die externe Authentisierung einer HPC oder einer SMC mit einer passenden Rollenennung im CHA-Feld des entsprechenden CV-Authentisierungszertifikats für Rollenauthentisierung (**C.HPC.AUTR_CVC** einer HPC oder **C.SMC.AUTR_CVC** einer SMC) erzielt, siehe **Tabelle (N2623.00)** in Annex A.3 von [HPC-P2].

Vor dem Authentisierungsprozess muss die SMC-A das CV-Zertifikat der Gegenseite prüfen, um den öffentlichen Schlüssel PuK.HPC.AUTR_CVC bzw. PuK.SMC.AUTR_CVC zu importieren.

Der durchzuführende Authentisierungsprozess entspricht dem zweiten Teil (HPC-Authentisierung) des Authentisierungsverfahrens zwischen HPC/eGK, das in Kapitel 6.4 von [HPC-P2] beschrieben ist.

Als erster Schritt der externen Authentisierung der autorisierenden Karte, wird der öffentliche Schlüssel für die Rollenauthentisierung der autorisierenden Karte zusammen mit dem passenden Algorithmus gesetzt.

Tabelle 25 - (N3027.00) MSE Kommando für die Schlüssel- und Algorithmenauswahl

CLA	Gemäß ISO/IEC 7816-4
INS	'22' = MANAGE SECURITY ENVIRONMENT
P1	'81' = SET für externe Authentisierung
P2	'A4' = Authentication Template im Datenfeld
Lc	'11' = Länge des zugehörigen Datenfeldes
Datenfeld	'83 0C xx ... xx' '80 01 00' = DO KeyRef von PuK.HPC.AUTR_CVC oder PuK.SMC.AUTR_CVC DO AlgID rsaRoleCheck
Le	Nicht vorhanden

Anmerkung – Als Schlüsselreferenz wird die CHR aus dem CV-Zertifikat der Gegenseite verwendet. Die Referenz hat eine Länge von 12 Bytes: Index '00' (1 Byte) || KeyRef von PrK.HPC.AUTR_CVC bzw. PrK.SMC.AUTR_CVC (1 Byte) || ICCSN der Gegenseite, d.h. ICCSN.HPC oder ICCSN.SMC (10 Bytes), siehe Kapitel 8.5.2 in [HPC-P1] zur CHR-Struktur.

Tabelle 26 - (N3028.00) MSE Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	'9000' oder spezifische Status-Bytes, siehe [HPC-P1]

Anschließend wird von der SMC-A eine Zufallszahl angefordert.

Tabelle 27 - (N3029.00) GET CHALLENGE Kommando

CLA	Gemäß ISO/IEC 7816-4
INS	'84' = GET CHALLENGE
P1, P2	'0000'
Lc	Nicht vorhanden
Datenfeld	Nicht vorhanden
Le	'08'

Tabelle 28 - (N3030.00) GET CHALLENGE Antwort

Datenfeld	RND.SMC (8 Bytes)
SW1-SW2	'9000' oder spezifische Status-Bytes, siehe [HPC-P1]

Die Zufallszahl wird zusammen mit den 8 LSB der ICCSN der SMC-A an die autorisierende Karte übergeben. Diese muss vor der Ausführung des INTERNAL AUTHENTICATE Kommandos den Sicherheitsstatus zur Nutzung ihres privaten Authentisierungsschlüssels (PrK.HPC.AUTR_CVC bzw. PrK.SMC.AUTR_CVC) durch eine geeignete Authentisierung gesetzt haben, d.h. eine Benutzerauthentisierung mit PIN.CH in der HPC oder eine externe Authentisierung mit entsprechender Rollenennung oder Benutzerauthentisierung mit PIN.SMC in der SMC-B. Das Ergebnis des Kommandos INTERNAL AUTHENTICATE ist eine digitale Signatur, die mit dem Kommando EXTERNAL AUTHENTICATE an die SMC-A übermittelt wird.

Tabelle 29 - (N3031.00) EXTERNAL AUTHENTICATE Kommando zur HPC- oder SMC-Authentisierung

CLA	Gemäß ISO/IEC 7816-4
INS	'82' = EXTERNAL AUTHENTICATE
P1	'00' = Algorithmus der Karte bereits bekannt
P2	'00' = Schlüsselreferenz der Karte bereits bekannt
Lc	'000100' = Länge des zugehörigen Datenfeldes = 256
Datenfeld	Auf die Authentisierung bezogene Daten, siehe Kapitel 14.7.1 in [HPC-P1]
Le	Nicht vorhanden

Tabelle 30 - (N3032.00) EXT. AUTHENTICATE Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	'9000' oder spezifische Status-Bytes, siehe [HPC-P1]

Die Authentisierungsdaten der autorisierenden Karte werden von der SMC-A geprüft. Falls die Authentisierung erfolgreich ist, wird in der SMC-A der Sicherheitsstatus zur Nutzung von PrK.SMC.AUTR_CVC gesetzt. Dieser private Schlüssel wird z.B. für die SMC/eGK-Interaktionen verwendet.

5.8 Interaktionen zwischen SMC-A und eGK

5.8.1 Asymmetrische SMC/eGK-Authentisierung ohne Aufbau eines Trusted Channel

Die SMC/eGK-Authentisierung wird in gleicher Weise wie die HPC/eGK-Authentisierung durchgeführt, siehe [Kapitel 6.4](#) in [HPC-P2], mit der SMC-A anstelle der HPC. Dazu wird der private Schlüssel für Rollenauthentisierung, PrK.SMC.AUTR_CVC, verwendet.

5.8.2 Asymmetrische SMC/eGK-Authentisierung mit Aufbau eines Trusted Channel

Falls zukünftige Anwendungen online eGK-Daten verarbeiten sollen, muss ein Trusted Channel zwischen einer eGK und einer SMC-A eingerichtet werden. Die Kommandos an der Schnittstelle zur SMC-A nach der CVC-Prüfung sind die gleichen wie für die SMC/eGK-Authentisierung ohne Aufbau eines Trusted Channel mit dem Unterschied, dass andere Algorithmenkennungen gesetzt werden.

Die RSA-Authentisierung mit Vereinbarung von Sitzungsschlüssel für SM muss als Algorithmus in der eGK gesetzt werden. Auf Seite der SMC-A ist die RSA-Authentisierung mit Vereinbarung von Sitzungsschlüsseln für Trusted Channel der entsprechend zu setzende Algorithmus.

5.9 Interaktionen zwischen SMC-A und HPC, SMC-B oder RFID-Token

5.9.1 Allgemeines

Kapitel 7.1 in [HPC-P2] gibt einen Überblick über die Authentisierungsprozesse, die zwischen SMC/HPC, SMC/SMC und SMC/RFID-Token möglich sind. Die SMC-A unterstützt ebenfalls das GET SECURITY STATUS KEY Kommando, mit dem z.B. der Authentisierungsstatus einer vorgegebenen Rollenkenennung von der Karte abgerufen werden kann; siehe Kapitel 7.2 in [HPC-P2].

Die SMC-A nutzt als entfernter PIN-Sender den entsprechenden privaten Schlüssel für die funktionale Geräteauthentisierung, PrK.SMC.AUTD_RPS_CVC, um mit einer HPC, einer SMC-B oder einem RFID-Token zu interagieren. Vor Ausführung der asymmetrischen Authentisierung müssen die CV-Zertifikate der SMC-A ausgelesen werden, siehe Kapitel 5.5.4. Die CV-Zertifikate der betroffenen Zielkarte (HPC, SMC-B bzw. RFID-Token) müssen geprüft werden, so dass die entsprechenden öffentlichen Schlüssel in der SMC-A verfügbar sind.

Da der private Schlüssel PrK.SMC.AUTD_RPS_CVC der SMC-A zum Senden der PIN durch eine externe Authentisierung einer zugehörigen HPC, einer SMC-B oder eines RFID-Token (welche die PIN empfangen) aktiviert werden, muss sich der jeweilige PIN-Empfänger zuerst authentisieren. Als Algorithmus wird in der SMC-A entweder die RSA-Authentisierung mit Vereinbarung von Sitzungsschlüsseln für Trusted Channel oder die Speicherung von Vorstellungsschlüsseln gesetzt.

5.9.2 Asymmetrische Authentisierung mit Aufbau eines Trusted Channel

Im ersten Teil des Verfahrens weist die HPC gegenüber der SMC-A seine Echtheit nach und aktiviert in der SMC-A den privaten Schlüssel PrK.SMC.AUTD_RPS_CVC. Bevor das Kommando für externe Authentisierung an die SMC-A gesendet wird, müssen die Referenz des öffentlichen Authentisierungsschlüssels der Zielkarte und die passende Algorithmenkennung gesetzt werden.

Tabelle 31 - (N3033.00) MSE Kommando für die Schlüssel- und Algorithmenauswahl

CLA	Gemäß ISO/IEC 7816-4
INS	'22' = MANAGE SECURITY ENVIRONMENT
P1	'81' = SET für externe Authentisierung
P2	'A4' = Authentication Template im Datenfeld
Lc	'11' = Länge des zugehörigen Datenfeldes
Datenfeld	'83 0C xx ... xx' '80 01 74' = DO KeyRef von PuK.HPC.AUTD_SUK_CVC (HPC) oder PuK.SMC.AUTD_RPE_CVC (SMC-B) oder PuK.KM.AUTD_RPE_CVC (RFID-Token), siehe Anmerkung DO AlgID rsaSessionkey4TC
Le	Nicht vorhanden

Anmerkung – Als Schlüsselreferenz wird die CHR aus dem CV-Zertifikat der Gegenseite verwendet. Die Referenz hat eine Länge von 12 Bytes: Index '00' (1 Byte) || KeyRef des privaten Schlüssels der Gegenseite (1 Byte) || ICCSN der Gegenseite (10 Bytes), siehe Kapitel 8.5.2 in [HPC-P1] zur CHR-Struktur.

Tabelle 32 - (N3034.00) MSE Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	'9000' oder spezifische Status-Bytes, siehe [HPC-P1]

Außerdem werden die Schlüsselreferenz für PrK.SMC.AUTD_RPS_CVC und eine passende Algorithmenkennung für die interne Authentisierung gesetzt.

Tabelle 33 - (N3035.00) MSE Kommando für die Schlüssel- und Algorithmenauswahl

CLA	Gemäß ISO/IEC 7816-4
INS	'22' = MANAGE SECURITY ENVIRONMENT
P1	'41' = SET für interne Authentisierung
P2	'A4' = Authentication Template im Datenfeld
Lc	'06' = Länge des zugehörigen Datenfeldes
Datenfeld	'84 01 10' '80 01 74' = DO KeyRef von PrK.SMC.AUTD_RPS_CVC DO AlgID rsaSessionkey4TC
Le	Nicht vorhanden

Tabelle 34 - (N3036.00) MSE Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	'9000' oder spezifische Status-Bytes, siehe [HPC-P1]

Anmerkung – Beide MSE SET Kommandos für externe und interne Authentisierung werden unmittelbar hintereinander ausgeführt, so dass die Sequenz der Authentisierungskommandos nicht durch ein MSE SET Kommando unterbrochen wird, siehe Kapitel 15 in [HPC-P1].

Anschließend fordert die externe Software von der SMC-A eine Zufallszahl an.

Tabelle 35 - (N3037.00) GET CHALLENGE Kommando

CLA	Gemäß ISO/IEC 7816-4
INS	'84' = GET CHALLENGE
P1, P2	'0000'
Lc	Nicht vorhanden
Datenfeld	Nicht vorhanden
Le	'08'

Tabelle 36 - (N3038.00) GET CHALLENGE Antwort

Datenfeld	RND.SMC (8 Bytes)
SW1-SW2	'9000' oder spezifische Status-Bytes, siehe [HPC-P1]

Die Zufallszahl wird zusammen mit den 8 LSB der ICCSN der Gegenseite übergeben. Das Ergebnis des von der Gegenseite ausgeführten Kommandos INTERNAL AUTHENTICATE ist eine digitale Signatur, die mit dem Kommando EXTERNAL AUTHENTICATE an die SMC-A zur Prüfung übermittelt wird.

Tabelle 37 - (N3039.00) EXT. AUTHENTICATE Kommando zur Authentisierung der Gegenseite

CLA	Gemäß ISO/IEC 7816-4
INS	'82' = EXTERNAL AUTHENTICATE
P1	'00' = Algorithmus der Karte bereits bekannt
P2	'00' = Schlüsselreferenz der Karte bereits bekannt
Lc	'000100' = Länge des zugehörigen Datenfeldes = 256
Datenfeld	Auf die Authentisierung bezogene Daten, siehe Kapitel 14.7.1 in [HPC-P1],
Le	Nicht vorhanden

Tabelle 38 - (N3040.00) EXT. AUTHENTICATE Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	'9000' oder spezifische Status-Bytes, siehe [HPC-P1]

Im zweiten Teil des Verfahrens weist die SMC-A der Gegenseite ihre Echtheit nach. Bevor das folgende Kommando an die SMC-A gesendet wird, fordert die externe Software von der Gegenseite eine Zufallszahl an.

Tabelle 39 - (N3041.00) INT. AUTHENTICATE Kommando

CLA	Gemäß ISO/IEC 7816-4
INS	'88' = INTERNAL AUTHENTICATE
P1	'00' = Algorithmus der Karte bereits bekannt
P2	'00' = Schlüsselreferenz der Karte bereits bekannt
Lc	'000010' = Länge des zugehörigen Datenfeldes
Datenfeld	Auf die Authentisierung bezogene Daten, siehe Kapitel 14.7.4 in [HPC-P1]
Le	'0100' = Länge der erwarteten Signatur

Tabelle 40 - (N3042.00) INT. AUTHENTICATE Antwort

Datenfeld	Auf die Authentisierung bezogene Daten, siehe Kapitel 14.7.4 in [HPC-P1],
SW1-SW2	'9000' oder spezifische Status-Bytes, siehe [HPC-P1]

Die Authentisierungsdaten aus dem Datenfeld der Antwort werden auf der entsprechenden Gegenseite geprüft. Dort wird der Sicherheitsstatus "CHA mit Profil 54 erfolgreich nachgewiesen" gesetzt.

Die auf die Authentisierung bezogenen Daten enthalten Elemente zur Schlüsselableitung. Die SM-Schlüssel werden gemäß Kapitel 13.1 in [HPC-P1] berechnet. Die Schlüssel werden dazu genutzt, SM-Datenobjekte zu generieren und zu verarbeiten, siehe Kapitel 5.9.5 bis Kapitel 5.9.8.

5.9.3 Asymmetrische Authentisierung mit Speicherung von Vorstellungsschlüsseln

In der Authentisierungssequenz mit Vereinbarung von Vorstellungsschlüsseln empfängt die Gegenseite das erste INTERNAL AUTHENTICATE und die SMC-A das erste EXTERNAL AUTHENTICATE, um in der SMC-A den Sicherheitsstatus zu setzen, der für die Verwendung des privaten Authentisie-

ungsschlüssels der SMC-A erforderlich ist. Bevor die Authentisierungskommandos zur SMC-A gesendet werden, müssen die Referenzen der Schlüssel und die passende Algorithmenkennungen für externe und interne Authentisierung gesetzt werden.

Beide MSE SET Kommandos für externe und interne Authentisierung werden unmittelbar hintereinander ausgeführt, so dass die Sequenz der Authentisierungskommandos nicht durch ein MSE SET Kommando unterbrochen wird, siehe Kapitel 15 in [HPC-P1].

Tabelle 41 - (N3043.00) MSE Kommando für die Schlüssel- und Algorithmenauswahl

CLA	Gemäß ISO/IEC 7816-4
INS	'22' = MANAGE SECURITY ENVIRONMENT
P1	'81' = SET für externe Authentisierung
P2	'A4' = Authentication Template im Datenfeld
Lc	'11' = Länge des zugehörigen Datenfeldes = 17
Datenfeld	'83 0C xx ... xx' '80 01 94' = DO KeyRef von PuK.HPC.AUTD_SUK_CVC (HPC) oder PuK.SMC.AUTD_RPE_CVC (SMC-B) oder PuK.KM.AUTD_RPE_CVC (RFID Token); siehe Anmerkung DO AlgID rsaSessionkey4Intro
Le	Nicht vorhanden

Anmerkung – Als Schlüsselreferenz wird die CHR aus dem CV-Zertifikat der Gegenseite verwendet. Die Referenz hat eine Länge von 12 Bytes: Index '00' (1 Byte) || KeyRef des privaten Schlüssels der Gegenseite (1 Byte) || ICCSN der Gegenseite (10 Bytes), siehe Kapitel 8.5.2 in [HPC-P1] zur CHR-Struktur.

Tabelle 42 - (N3044.00) MSE Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	'9000' oder spezifische Status-Bytes; siehe [HPC-P1]

Tabelle 43 - (N3045.00) MSE Kommando für die Schlüssel- und Algorithmenauswahl

CLA	Gemäß ISO/IEC 7816-4
INS	'22' = MANAGE SECURITY ENVIRONMENT
P1	'41' = SET für interne Authentisierung
P2	'A4' = Authentication Template im Datenfeld
Lc	'06' = Länge des zugehörigen Datenfeldes = 6
Datenfeld	'84 01 12' '80 01 94' = DO KeyRef von PrK.SMC.AUTD_RPS_CVC der SMC DO AlgID rsaSessionkey4Intro
Le	Nicht vorhanden

Tabelle 44 - (N3046.00) MSE Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	'9000' oder spezifische Status-Bytes; siehe [HPC-P1]

Der erste Teil des Verfahrens umfasst die Authentisierung der Gegenseite. Zunächst wird von der SMC-A eine Zufallszahl angefordert. Dann muss ein INTERNAL AUTHENTICATE mit RND.SMC || ICCSN8.SMC im Datenfeld an die Gegenseite gesendet werden. Das Ergebnis der digitalen Signatur wird mit dem Kommando EXTERNAL AUTHENTICATE an die SMC-A zur Prüfung übermittelt.

Tabelle 45 - (N3047.00) GET CHALLENGE Kommando

CLA	Gemäß ISO/IEC 7816-4
INS	'84' = GET CHALLENGE
P1, P2	'0000'
Lc	Nicht vorhanden
Datenfeld	Nicht vorhanden
Le	'08'

Tabelle 46 - (N3048.00) GET CHALLENGE Antwort

Datenfeld	RND.SMC (8 Bytes)
SW1-SW2	'9000' oder spezifische Status-Bytes; siehe [HPC-P1]

Tabelle 47 - (N3049.00) EXTERNAL AUTHENTICATE Kommando

CLA	Gemäß ISO/IEC 7816-4
INS	'82' = EXTERNAL AUTHENTICATE
P1	'00' = Algorithmus der Karte bereits bekannt
P2	'00' = Key Reference der Karte bereits bekannt
Lc	'000100' = Länge des nachfolgenden Datenfeldes = 256
Datenfeld	Auf die Authentisierung bezogene Daten, siehe Kapitel 14.7.1 in [HPC-P1]
Le	Nicht vorhanden

Tabelle 48 - (N3050.00) EXTERNAL AUTHENTICATE Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	'9000' oder spezifische Status-Bytes; siehe [HPC-P1]

Wenn die Authentisierung erfolgreich ist, setzt die SMC-A vorübergehend den Sicherheitsstatus, der für die Nutzung des Authentisierungsschlüssels PrK.SMC.AUTD_RPS_CVC notwendig ist. Die auf die Authentisierung bezogenen Daten enthalten Elemente zur Schlüsselableitung. Im zweiten Teil des Verfahrens weist die SMC-A gegenüber der Gegenseite ihre Echtheit nach. Dazu muss die externe Software von der Gegenseite eine Zufallszahl anfordern. Die Zufallszahl wird der SMC-A zusammen mit den 8 LSB der ICCSN der Gegenseite im folgenden INTERNAL AUTHENTICATE Kommando übergeben.

Tabelle 49 - (N3051.00) INTERNAL AUTHENTICATE Kommando

CLA	Gemäß ISO/IEC 7816-4
INS	'88' = INTERNAL AUTHENTICATE
P1	'00' = Algorithmus der Karte bereits bekannt
P2	'00' = Schlüsselreferenz der Karte bereits bekannt
Lc	'000010' = Länge des zugehörigen Datenfeldes = 16
Datenfeld	Auf die Authentisierung bezogene Daten, siehe Kapitel 14.7.4 von [HPC-P1]
Le	'0100' = Länge der erwarteten Signatur = 256

Tabelle 50 - (N3052.00) INTERNAL AUTHENTICATE Antwort

Datenfeld	Auf die Authentisierung bezogene Daten, siehe Kapitel 14.7.4 von [HPC-P1]
SW1-SW2	'9000' oder spezifische Status-Bytes; siehe [HPC-P1]

Die berechnete digitale Signatur wird der Gegenseite in einem EXTERNAL AUTHENTICATE Kommando übermittelt.

Gemäß Kapitel 13.1 in [HPC-P1] werden während des ersten Kommandos, das auf die Authentisierungssequenz folgt, die Vorstellungsschlüssel abgeleitet und deren Attribute gesetzt. Die CHR aus dem CV-Zertifikat der Gegenseite wird als Schlüsselreferenz gespeichert, nachdem der Index (erstes Byte der CHR) an das berechnete Schlüsselmaterial angepasst wurde, d.h. '02' für 3TDES-Schlüssel, siehe Kapitel 8.5.2 in [HPC-P1]. Während der Ableitung der Vorstellungsschlüssel wird der Sicherheitsstatus gelöscht, Secure Messaging wird nicht eingeschaltet. Die Vorstellungsschlüssel werden in einer symmetrischen Authentisierung verwendet, um Sitzungsschlüssel für Trusted Channel zu vereinbaren, siehe nächstes Kapitel.

5.9.4 Symmetrische Authentisierung mit Aufbau eines Trusted Channel

Falls eine bestimmte SMC-A und eine bestimmte HPC (oder SMC-B oder RFID-Token) sich bereits einander vorgestellt, d.h. eine asymmetrische Authentisierung mit persistenter Speicherung von Vorstellungsschlüsseln durchgeführt haben, können beide Karten unter Nutzung der gemeinsamen Vorstellungsschlüssel die symmetrische Authentisierung ausführen.

Bei erfolgreicher symmetrischer Authentisierung wird der Sicherheitsstatus "Erfolgreiche Prüfung der Rollenkenntung der HPC (bzw. der SMC-B oder des RFID-Token)" gesetzt, da die nachgewiesene Rollenkenntung, die verwendete Schlüsselkenntung und die Zugriffsregel des privaten Schlüssels auf die Vorstellungsschlüssel übergegangen sind, siehe [HPC-P1], Kapitel 8.5.2, Kapitel 13.1.1 und Kapitel 15.6.

Die Kommandosequenz auf Seite der SMC-A beginnt mit dem Auswählen der Vorstellungsschlüssel und der entsprechenden Algorithmenkenntung für gegenseitige Authentisierung.

Tabelle 51 - (N3053.00) MSE Kommando für die Schlüssel- und Algorithmenauswahl

CLA	Gemäß ISO/IEC 7816-4
INS	'22' = MANAGE SECURITY ENVIRONMENT
P1	'81' = SET für gegenseitige Authentisierung
P2	'A4' = Authentication Template im Datenfeld
Lc	'11' = Länge des zugehörigen Datenfeldes
Datenfeld	'83 0C 02 xx ... xx' '80 01 74' = DO KeyRef der Vorstellungsschlüssel (3TDES) DO AlgID des Sessionkey4TC
Le	Nicht vorhanden

Tabelle 52 - (N3054.00) MSE Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	'9000' oder spezifische Status-Bytes, siehe [HPC-P1]

Anmerkung – Die Schlüsselreferenz hat eine Länge von 12 Bytes: Index '02' für 3TDES (1 Byte) || KeyRef von PrK.HPC.AUTD_SUK_CVC der HPC oder PrK.SMC.AUTD_RPE_CVC der SMC-B oder PrK.KM.AUTD_RPE_CVC des RFID-Token (1 Byte) || ICCSN der Gegenseite (10 Bytes), siehe Kapitel 8.5.2 in [HPC-P1] zum Aufbau der Referenz von Vorstellungsschlüsseln.

Anschließend wird eine Zufallszahl von der SMC-A abgerufen.

Tabelle 53 - (N3055.00) GET CHALLENGE Kommando

CLA	Gemäß ISO/IEC 7816-4
INS	'84' = GET CHALLENGE
P1, P2	'0000'
Lc	Nicht vorhanden
Datenfeld	Nicht vorhanden
Le	'08'

Tabelle 54 - (N3056.00) GET CHALLENGE Antwort

Datenfeld	RND.SMC (8 Bytes)
SW1-SW2	'9000' oder spezifische Status-Bytes, siehe [HPC-P1]

Nach dem GET CHALLENGE Kommando wird ein INTERNAL AUTHENTICATE Kommando mit RND.SMC || ICCSN8.SMC im Datenfeld an die Gegenseite gesendet. Anschließend folgt auf Seite der SMC-A ein MUTUAL AUTHENTICATE Kommando. Dieses Kommando übermittelt die Authentisierungsdaten der Gegenseite an die SMC-A. Die SMC-A prüft die Daten der Gegenseite und berechnet die eigenen Authentisierungsdaten.

Tabelle 55 – (N3057.00) MUTUAL AUTHENTICATE Kommando

CLA	Gemäß ISO/IEC 7816-4
INS	'82' = MUTUAL AUTHENTICATE
P1	'00' = Algorithmus der Karte bereits bekannt
P2	'00' = Schlüsselreferenz der Karte bereits bekannt
Lc	'68' = Länge des zugehörigen Datenfeldes = 104
Datenfeld	Auf die Authentisierung bezogene Daten, siehe Kapitel 14.7.1 in [HPC-P1]
Le	'68' = Länge der erwarteten Authentisierungsdaten = 104

Tabelle 56 - (N3058.00) MUTUAL AUTHENTICATE Antwort

Datenfeld	Auf die Authentisierung bezogene Daten, siehe Kapitel 14.7.1 in [HPC-P1]
SW1-SW2	'9000' oder spezifische Status-Bytes, siehe [HPC-P1]

Die Authentisierungsdaten der SMC-A (aus dem Datenfeld der Antwort) werden in der entsprechenden Zielkarte mittels EXTERNAL AUTHENTICATE Kommando geprüft. Die erfolgreiche Prüfung setzt in der Zielkarte (HPC, SMC-B oder RFID-Token) den Sicherheitsstatus "CHA mit Profil 54 erfolgreich nachgewiesen", siehe [Tabelle \(N2624.00\)](#) in Annex A.3 von [HPC-P2]. Ein Trusted Channel steht nun zur Verfügung, in dem die Daten mit Secure Messaging zur Gegenseite übertragen werden.

5.9.5 Erzeugen gesicherter Kommandos mit PSO-Kommandos

Die Unterstützung von PSO-Kommandos zur Erzeugung und Prüfung von SM-Datenobjekten ist obligatorisch, siehe Kapitel 14.8 in [HPC-P1]. Die Unterstützung des Kommandos ENVELOPE, das in [Kapitel 5.9.7](#) spezifiziert wird, ist optional. Das ENVELOPE Kommando ist ein alternatives Verfahren HPC-Spezifikation V2.3.2, Teil III

zur Unterstützung des Trusted Channel. Das Datenobjekt Card Capabilities in EF.ATR (siehe Tabelle 4 (N3005.00)) zeigt an, ob ausschließlich das erste oder beide Verfahren unterstützt werden. Die generellen Vorgaben für die Unterstützung eines Trusted Channel und die PSO-Kommandos sind in den Kapiteln 13.2, 13.3 und 14.8 von [HPC-P1] beschrieben. Zur Erstellung der SM-Datenobjekte werden die folgenden Kommandos verwendet:

- PSO: COMPUTE CRYPTOGRAPHIC CHECKSUM
- PSO: ENCIPHER

Alle Kommandos werden ohne Secure Messaging gesendet, da die SMC-A keine SM-Kommandos verarbeitet, sondern Datenobjekte für Secure Messaging erzeugt. und die Sitzungsschlüssel sozusagen als Benutzerschlüssel betrachtet. Weil sowohl die Schlüssel für MAC-Berechnung und Verschlüsselung, als auch die zu verwendenden Algorithmen implizit bekannt sind, brauchen keine Schlüsselreferenzen oder Algorithmenkennungen gesetzt zu werden.

Tabelle 57 – (N3059.00) PSO: COMPUTE CRYPTOGRAPHIC CHECKSUM Kommando

CLA	Gemäß ISO/IEC 7816-4
INS	'2A' = PSO: COMPUTE CRYPTOGRAPHIC CHECKSUM
P1	'8E' = CC im Datenfeld der Antwort
P2	'80' = PV im Datenfeld des Kommandos
Lc	'xx' oder '00xxxx' = Länge des zugehörigen Datenfeldes
Datenfeld	Daten, für die die kryptografische Prüfsumme berechnet werden soll (Kommando der Zielkarte möglicherweise mit einem der Datenobjekte PV, Le oder CG, siehe auch Anmerkung)
Le	'00' oder '0000'

Anmerkung – Die speziellen Padding-Regeln, wie sie in Kapitel "Cryptographic checksum data element" von ISO/IEC 7816-4, beschrieben werden, müssen bei der Erzeugung der Daten für das Datenfeld des Kommandos berücksichtigt werden, d.h. die Padding-Bytes müssen eingefügt werden, siehe Kommandobeschreibung in Kapitel 14.8.2 von [HPC-P1].

Tabelle 58 – (N3060.00) PSO: COMPUTE CRYPTOGRAPHIC CHECKSUM Antwort

Datenfeld	Kryptografische Prüfsumme
SW1-SW2	'9000' oder spezifische Status-Bytes, siehe [HPC-P1]

Wenn in dem gesicherten Kommando der Zielkarte verschlüsselte Daten transportiert werden müssen (z.B. eine PIN), wird die Berechnung des Kryptogramms mit dem Kommando PSO: ENCIPHER durchgeführt, das vor dem Kommando PSO: COMPUTE CRYPTOGRAPHIC CHECKSUM gesendet werden muss.

Tabelle 59 – (N3061.00) PSO: ENCIPHER Kommando

CLA	Gemäß ISO/IEC 7816-4
INS	'2A' = PSO: ENCIPHER
P1	'86' = Padding Indicator Kryptogramm im Datenfeld der Antwort
P2	'80' = PV im Datenfeld des Kommandos
Lc	'xx' oder '00xxxx' = Länge des zugehörigen Datenfeldes
Datenfeld	Zu verschlüsselnde Daten
Le	'00' oder '0000'

Tabelle 60 – (N3062.00) PSO: ENCIPHER Antwort

Datenfeld	'01' (Padding Indicator) verschlüsselte Daten
SW1-SW2	'9000' oder spezifische Status-Bytes, siehe [HPC-P1]

5.9.6 Verarbeiten gesicherter Antworten mit PSO-Kommandos

Zur Prüfung einer kryptografischen Prüfsumme muss die PSO-Operation VERIFY CRYPTOGRAPHIC CHECKSUM verwendet werden.

Tabelle 61 – (N3063.00) PSO: VERIFY CRYPTOGRAPHIC CHECKSUM Kommando

CLA	Gemäß ISO/IEC 7816-4
INS	'2A' = PSO: VERIFY CRYPTOGRAPHIC CHECKSUM
P1	'00'
P2	'A2' = PV im Datenfeld des Kommandos
Lc	'xx' oder '00xxxx' = Länge des zugehörigen Datenfeldes
Datenfeld	'80'-L-PV '8E'-L-CC
Le	Nicht vorhanden

Tabelle 62 – (N3064.00) PSO: VERIFY CRYPTOGRAPHIC CHECKSUM Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	'9000' oder spezifische Status-Bytes, siehe [HPC-P1]

Wenn die Antwortdaten ein Kryptogramm enthalten, dann werden die entschlüsselten Daten mit der PSO-Operation DECIPHER abgerufen.

Tabelle 63 – (N3065.00) PSO: DECIPHER Kommando

CLA	Gemäß ISO/IEC 7816-4
INS	'2A' = PSO: DECIPHER
P1	'80' = PV im Datenfeld der Antwort
P2	'86' = Padding Indicator Kryptogramm im Datenfeld des Kommandos
Lc	'xx' oder '00xxxx' = Länge des zugehörigen Datenfeldes
Datenfeld	'01' (Padding Indicator) Kryptogramm
Le	'00' oder '0000'

Tabelle 64 – (N3066.00) PSO: DECIPHER Antwort

Datenfeld	Entschlüsselte Daten
SW1-SW2	'9000' oder spezifische Status-Bytes, siehe [HPC-P1]

5.9.7 Erzeugen gesicherter Kommandos mit ENVELOPE (optional)

In diesem Fall wird das zu sichernde Kommando im Datenfeld des ENVELOPE-Kommandos an die SMC-A geschickt, um das DO kryptografische Prüfsumme (CC) und bei Bedarf auch das DO Kryptogramm (CG) mit der Antwort abzurufen. Damit kann die zur Erzeugung eines gesicherten Kommandos benötigte Zeit möglicherweise reduziert werden. Zu diesem Zweck wird ein ENVELOPE-Kommando HPC-Spezifikation V2.3.2, Teil III

mit ungeradem Instruction Code im ungesicherten Modus an die SMC geschickt, d.h. die SMC-A kann das ENVELOPE-Kommando verarbeiten. Das Kommando ist in Kapitel 14.9.1 von [HPC-P1] beschrieben.

Im Datenfeld sind das Datenobjekt 'Command-to-perform' (Tag '52') mit dem ungesicherten Kommando und das SM-Template (Tag '7D') vorhanden; letzteres enthält den "Response Descriptor", der angibt, was zurückgegeben werden soll: das SM-Datenobjekt CC und – falls benötigt – auch das SM-Datenobjekt CG, gekapselt in einem SM-Template. Das SM-Template erzwingt die Nutzung von SM-Schlüsseln.

Anmerkung – Das Kommando ENVELOPE mit ungeradem Instruction Code erlaubt die Ausführung derartiger Leistungen.

Tabelle 65 – (N3067.00) ENVELOPE Kommando zum Erzeugen von SM-Datenobjekten eines gesicherten Kommandos

CLA	Gemäß ISO/IEC 7816-4
INS	'C3' = ENVELOPE
P1-P2	'0000'
Lc	'xx' oder '00xxxx' = Länge des zugehörigen Datenfeldes
Datenfeld	- Case 1: Wenn das zu sichernde Kommando Daten enthält, die als DO PV übertragen werden sollen: '52'-L- abzusicherndes Kommando '7D'-L-('BA' -L- ['8E'-'00']) - Case 2: Wenn das zu sichernde Kommando Daten enthält, die als DO CG übertragen werden sollen: '52'-L- abzusicherndes Kommando, das abzusichern ist '7D'-L-('BA' -L- ['87'-'00' '8E'-'00'])
Le	'00' oder '0000'

Tabelle 66 – (N3068.00) ENVELOPE Antwort

Datenfeld	- Case 1: '7D'-L-('8E' -'08'-CC) - Case 2: '7D'-L-('87' -L- '01'-CG '8E' -'08'-CC)
SW1-SW2	'9000' oder spezifische Status-Bytes, siehe [HPC-P1]

Das Wertefeld des DO 'Command-to-perform' (Tag '52') muss in die Berechnung der CC eingehen. Dabei müssen die Regeln für die CC-Berechnung für SM-geschützte Kommandos, wie sie in [ISO7816-4] definiert sind, angewendet werden. Der Kommando-Header muss dabei immer in die CC integriert sein.

5.9.8 Verarbeiten gesicherter Antworten mit ENVELOPE (optional)

Zur Verarbeitung einer gesicherten Antwort-APDU sind 3 Fälle zu unterscheiden:

- Antwort mit DO Status-Bytes (Tag '99')
- Antwort mit DO Klartext (Tag '81') und DO Status-Bytes (Tag '99')
- Antwort mit DO Kryptogramm (Tag '87') und DO Status-Bytes (Tag '99').

Anmerkung – Die hier beschriebenen Fälle sind Anwendungsfälle und sollten nicht mit den Fällen von Kommando-Antwort-Paaren der Datenübertragung, wie sie in ISO/IEC 7816-3 beschrieben sind, verwechselt werden.

Jede Antwort ist mit einer kryptografischen Prüfsumme CC gesichert. Die CC muss geprüft werden. Falls ein Kryptogramm vorhanden ist, muss der Klartext durch die SMC-A nach erfolgreicher Prüfung der CC zurückgeliefert werden. Das Kommando ist in Kapitel 14.9.1 von [HPC-P1] beschrieben.

Tabelle 67 – (N3069.00) ENVELOPE Kommando zur Verarbeitung von SM-DOs einer gesicherten Antwort

CLA	Gemäß ISO/IEC 7816-4
INS	'C3' = ENVELOPE
P1-P2	'0000'
Lc	'xx' oder '00xxxx' = Länge des zugehörigen Datenfeldes
Datenfeld	<ul style="list-style-type: none"> - Case 1: Antwort-APDU mit DO Processing status und DO CC: '7D'-L-('99'-'02'- SW1-SW2 '8E'-'08'-CC) - Case 2: Antwort-APDU mit DO Plain Value, DO Processing status und DO CC: '7D'-L-('81'-L- Daten '99'-'02'- SW1-SW2 '8E'-'08'-CC) - Case 3: Antwort-APDU mit DO Cryptogram, DO Processing status und DO CC: '7D'-L-('87'-L- '01'-CG '99'-'02'- SW1-SW2 '8E'-'08'-CC 'BA' -L- ['80'-'00'])
Le	Case 1, 2: Nicht vorhanden Case 3: '00' oder '0000'

Tabelle 68 – (N3070.00) ENVELOPE Antwort

Datenfeld	<ul style="list-style-type: none"> - Case 1: Nicht vorhanden - Case 2: Nicht vorhanden - Case 3: '7D'- L-('80'-L-entschlüsselte Daten)
SW1-SW2	'9000' oder spezifische Status-Bytes, siehe [HPC-P1]

5.10 Die Sicherheitsmodul-Anwendung

5.10.1 Dateistruktur und Dateiinhalt

Die folgende Abbildung zeigt die Dateistruktur von DF.SMA für eine SMC-A.

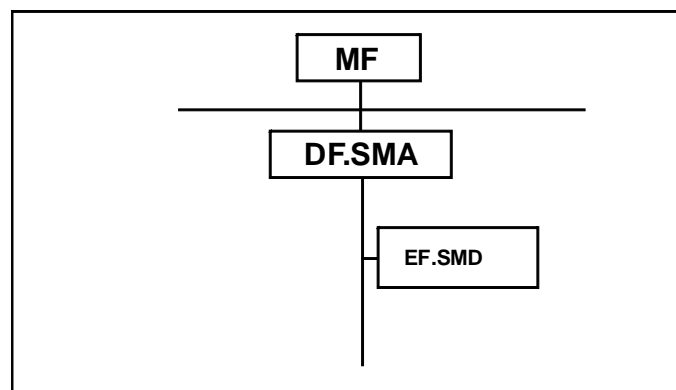


Abbildung 3 – (N3071.00) Dateistruktur von DF.SMA einer SMC-A

Im DF.SMA der SMC-A gibt es weder ein EF.CONF noch ein EF.NET.

5.10.1.1 DF.SMA (Security Module Application)

DF.SMA ist ein „Application Directory“ gemäß Kapitel 8.3.1.1 in [HPC-P1] d.h. ist mittels Anwendungskennung auszuwählen. Tabelle 69 (N3072.00) zeigt die Eigenschaften des Anwendungsverzeichnis.

Tabelle 69 – (N3072.00) Attribute von MF / DF.SMA

Attribut	Wert	Anmerkung
Objekttyp	Application Directory	
Application Identifier	'D27600014605'	
File Identifier	-	Herstellerspezifisch; Falls unterstützt, dann außerhalb des Intervalls ['1000', 'FEFF']; siehe Kapitel 8.1.1 in [HPC-P1]
Life Cycle Status	Operational State (activated)	
Zugriffsregel in allen SEs		
Zugriffsart	Sicherheitsbedingung	Anmerkung
SELECT	ALWAYS	
LOAD APPLICATION (nach Ausgabe der SMC-A)	AUT('D27600014600' '01') AND SmMac AND SmCmdEnc	Nur ausführbar, wenn ein CAMS genutzt wird, siehe Kapitel 5.12. Falls ein CAMS mit symmetrischer Authentisierung eingesetzt wird, muss die Sicherheitsbedingung die Schlüsselreferenz des entsprechenden symmetrischen Schlüssels enthalten, d.h. AUT('13') statt AUT('D27600014600' '01')
ACTIVATE, DEACTIVATE, DELETE	NEVER	

Die Schlüssel und CV-Zertifikate für den Authentisierungsprozess sind auf MF-Ebene lokalisiert. Die Sicherheitsmodul-Anwendung erlaubt das Anlegen weiterer Dateien, falls dafür in der Zukunft eine Notwendigkeit bestehen sollte, siehe Kapitel 5.12.

5.10.1.2 EF.SMD

Die transparente Datei EF.SMD ist für die Speicherung von SMC-A-bezogenen Daten vorgesehen, z.B. von speziellen Konfigurationsdaten. Die Datei kann immer gelesen werden, aber eine Aktualisierung ist nur nach erfolgreicher Authentisierung zwischen der SMC-A und einer entsprechenden HPC oder SMC möglich. Die folgende Tabelle zeigt die Attribute und Zugriffsbedingungen der Datei EF.SMD.

Tabelle 70 – (N3073.00) Attribute von MF / DF.SMA / EF.SMD

Attribut	Wert	Anmerkung
Objekttyp	Transparent Elementary File	
File Identifier	'D001'	
Short File Identifier	'01' = 1	
Number of Bytes	1024	
Flag Transaction Mode	False	
Flag Checksum	True	
Life Cycle Status	Operational State (activated)	
Content	...	
Zugriffsregel in allen SEs		
Zugriffsart	Sicherheitsbedingung	Anmerkung
SELECT, READ BINARY	ALWAYS	
UPDATE BINARY, ERASE BINARY	AUT('D27600004000' 'xx')	Rollenauthentisierung einer HPC oder einer SMC mit zugehörigem persönlichen Profil, z.B. Profil 2, siehe [HPC-P2], Tabelle (N2623.00) .
ACTIVATE, DEACTIVATE, DELETE	NEVER	

5.10.2 Sicherheitsumgebungen auf DF-Ebene

In DF.SMA wird nur das voreingestellte SE # 1 verwendet. Es ist möglich, in SE # 1 einen Trusted Channel aufzubauen, um z.B. Daten in zukünftigen Anwendungen online zu bearbeiten.

5.10.3 Auswahl der Anwendung

Die Auswahl der Anwendung wird mit dem ISO/IEC 7816-4 SELECT Kommando erzielt wie in den folgenden Tabellen angegeben.

Tabelle 71 - (N3074.00) SELECT Kommando zur Auswahl von DF.SMA

CLA	Gemäß ISO/IEC 7816-4
INS	'A4' = SELECT
P1	'04' = DF-Auswahl mittels AID
P2	'0C' = Keine FCI in der Antwort
Lc	'06' = Länge des zugehörigen Datenfeldes
Datenfeld	'D27600014605' = AID von DF.SMA einer SMC-A
Le	Nicht vorhanden

Tabelle 72 - (N3075.00) SELECT Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	'9000' oder spezifische Status-Bytes, siehe [HPC-P1]

5.10.4 Lesen, Aktualisieren und Löschen von Daten in EF.SMD

Zum Lesen von EF.SMD wird das ISO/IEC 7816-4 Kommando READ BINARY verwendet.

Tabelle 73 - (N3076.00) READ BINARY Kommando mit SFID zum Lesen von EF.SMD

CLA	Gemäß ISO/IEC 7816-4
INS	'B0' = READ BINARY
P1, P2	- P1 = b8-b6: 100 b5-b1: 0001 SFID von EF.SMD: 1 P2 = Offset - 'xxxx' = Offset (bit b8 von P1 = 0)
Lc	Nicht vorhanden
Datenfeld	Nicht vorhanden
Le	'00' oder '000000' = Lesen bis zum Ende der Datei

Tabelle 74 - (N3077.00) READ BINARY Antwort

Datenfeld	Daten
SW1-SW2	'9000' oder spezifische Status-Bytes, siehe [HPC-P1]

Falls die unterstützte „Extended Length“ nicht ausreicht, um die Daten mit einem einzelnen Befehl zu lesen, muss das READ BINARY Kommando mit Angabe des entsprechenden Offsets in P1-P2 wiederholt werden.

Zum Aktualisieren von EF.SMD dient das ISO/IEC 7816-4 Kommando UPDATE BINARY. Der für die Schreiboperation erforderliche Sicherheitsstatus ist die erfolgreiche Authentisierung einer HPC oder einer SMC, siehe Tabelle 70 (N3073.00).

Tabelle 75 - (N3078.00) UPDATE BINARY Kommando zum Aktualisieren von EF.SMD

CLA	Gemäß ISO/IEC 7816-4
INS	'D6' = UPDATE BINARY
P1, P2	- P1 = b8-b6: 100 b5-b1: 00001 SFID von EF.SMD: 1 P2 = Offset - 'xxxx' = Offset (bit b8 von P1 = 0)
Lc	'xx' oder '00xxxx' = Länge des zugehörigen Datenfeldes
Datenfeld	Daten
Le	Nicht vorhanden

Tabelle 76 - (N3079.00) UPDATE BINARY Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	'9000' oder spezifische Status-Bytes, siehe [HPC-P1]

Falls die unterstützte „Extended Length“ nicht ausreicht, um die Daten mit einem einzelnen Befehl zu schreiben, muss das UPDATE BINARY Kommando mit Angabe des entsprechenden Offsets in P1-P2 wiederholt werden.

Zum Löschen von Daten in EF.SMD wird das ISO/IEC 7816-4 Kommando ERASE BINARY verwendet, siehe Tabelle 77 (N3080.00). Das Kommando löscht Daten, indem es die Daten-Bytes mit '00'-Bytes überschreibt, siehe Kapitel 14.3.1 in [HPC-P1]. Der für die Löschoption erforderliche Sicherheitsstatus ist die erfolgreiche HPC- oder SMC-Authentisierung, siehe Tabelle 70 (N3073.00).

Tabelle 77- (N3080.00) ERASE BINARY Kommando zum Löschen von Daten in EF.SMD

CLA	Gemäß ISO/IEC 7816-4
INS	'0E' = ERASE BINARY
P1, P2	- P1 = b8-b6: 100 b5-b1: 00001 SFID von EF.SMD: 1 P2 = Offset - 'xxxx' = Offset (bit b8 von P1 = 0)
Lc	Nicht vorhanden
Datenfeld	Nicht vorhanden
Le	Nicht vorhanden

Tabelle 78 - (N3081.00) ERASE BINARY Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	'9000' oder spezifische Status-Bytes, siehe [HPC-P1]

Falls die unterstützte „Extended Length“ nicht ausreicht, um die Daten mit einem einzelnen Befehl zu löschen, muss das ERASE BINARY Kommando mit Angabe des entsprechenden Offsets in P1-P2 wiederholt werden.

5.11 Die KT-Anwendung (Kartenterminal-Anwendung)

5.11.1 Dateistruktur und Dateiinhalt

DF.KT wird verwendet für:

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

Die folgende Abbildung zeigt die Dateistruktur von DF.KT für die SMC-A.

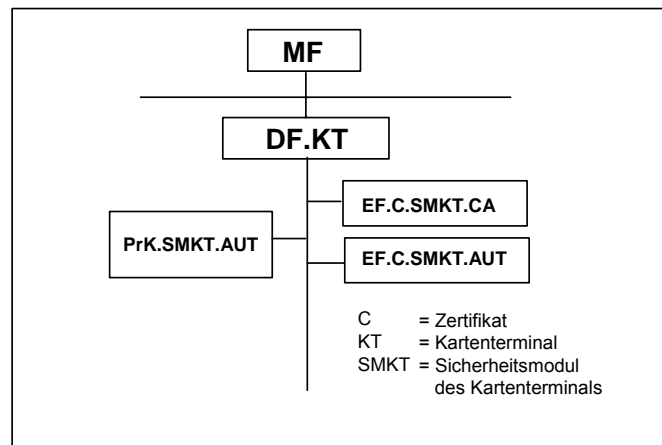


Abbildung 4 – (N3082.00) Dateistruktur von DF.KT

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

5.11.1.1 DF.KT (Kartenterminal-Anwendung)

DF.KT ist ein "Application Directory" gemäß Kapitel 8.3.1.1 in [HPC-P1], d.h. ist mittels Anwendungskennung auszuwählen. Tabelle 79 (N3083.00) zeigt die Eigenschaften des Anwendungsverzeichnisses.

Tabelle 79 – (N3083.00) Attribute von MF / DF.KT

Attribut	Wert	Anmerkung
Objekttyp	Application Directory	
Application Identifier	'D27600014400'	Anwendung der gematik
File Identifier	-	Herstellerspezifisch; Falls unterstützt, dann außerhalb des Intervalls ['1000', 'FEFF']; siehe Kapitel 8.1.1 in [HPC-P1]
Life Cycle Status	Operational State (activated)	
Zugriffsregel in allen SEs		
Zugriffsart	Sicherheitsbedingung	Anmerkung
SELECT	ALWAYS	
LOAD APPLICATION, ACTIVATE, DEACTIVATE, DELETE	NEVER	

5.11.1.2 EF.C.SMKT.CA

Die Datei EF.C.SMKT.CA enthält das X.509-Zertifikat der Zertifizierungsinstanz, die das X.509-Zertifikat C.SMKT.AUT ausgegeben hat. In Tabelle 80 (N3084.00) sind die Dateikennungen und Zugriffsbedingungen dargestellt.

Tabelle 80 – (N3084.00) Attribute von MF / DF.KT / EF.C.SMKT.CA

Attribut	Wert	Anmerkung
Objektyp	Transparent Elementary File	
File Identifier	'C502'	
Short File Identifier	'02' = 2	
Number of Bytes	1536 oder auf Zertifikatslänge beschränkt	
Flag Transaction Mode	False	
Flag Checksum	False	
Life Cycle Status	Operational State (activated)	
Content	...	Wird personalisiert
Zugriffsregel in allen SEs		
Zugriffsart	Sicherheitsbedingung	Anmerkung
SELECT, READ BINARY	ALWAYS	
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, UPDATE BINARY	NEVER	

5.11.1.3 EF.C.SMKT.AUT

Die Datei EF.C.SMKT.AUT enthält das X.509-Authentisierungszertifikat. In Tabelle 81 (N3085.00) sind die Dateikennungen und Zugriffsbedingungen dargestellt.

Tabelle 81 – (N3085.00) Attribute von MF / DF.KT / EF.C.SMKT.AUT

Attribut	Wert	Anmerkung
Objektyp	Transparent Elementary File	
File Identifier	'C501'	
Short File Identifier	'01' = 1	
Number of Bytes	1536 oder auf Zertifikatslänge beschränkt	
Flag Transaction Mode	False	
Flag Checksum	False	
Life Cycle Status	Operational State (activated)	
Content	...	Wird personalisiert
Zugriffsregel in allen SEs		
Zugriffsart	Sicherheitsbedingung	Anmerkung
SELECT, READ BINARY	ALWAYS	
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, UPDATE BINARY	NEVER	

5.11.1.4 PrK.SMKT.AUT

PrK.SMKT.AUT ist der private Authentisierungsschlüssel zur Anbindung des Kartenterminals an einen bestimmten Konnektor. Die Eigenschaften des Schlüssels sind in der nachfolgenden Tabelle angegeben.

Tabelle 82 – (N3086.00) Attribute von MF / DF.KT / PrK.SMKT.AUT

Attribut	Wert	Anmerkung
Objektyp	Privates RSA-Objekt	
Key Identifier	'02' = 2	
Key Reference	'82'	
Private Key (2048 Bits)	Wird personalisiert
Key Available	True	
Algorithm Identifier	rsaDecipherPKCS1_V1_5 signPKCS1_V1_5	
Zugriffsregel in allen SEs		
Zugriffsart	Sicherheitsbedingung	Anmerkung
PSO: DECIPHER	ALWAYS	
INTERNAL AUTHENTICATE	ALWAYS	
Andere	NEVER	

5.11.2 Sicherheitsumgebungen auf DF-Ebene

In DF.KT wird nur das SE # 1 (Default-SE) verwendet. Es ist möglich, in SE # 1 einen Trusted Channel aufzubauen, um z.B. Daten in zukünftigen Anwendungen online zu bearbeiten.

5.11.3 Auswahl der Anwendung

Die Auswahl der Anwendung wird mit dem ISO/IEC 7816-4 SELECT Kommando durchgeführt wie in den folgenden zwei Tabellen angegeben.

Tabelle 83 - (N3087.00) SELECT Kommando zur Auswahl der KT-Anwendung

CLA	Gemäß ISO/IEC 7816-4
INS	'A4' = SELECT
P1	'04' = DF-Auswahl mittels AID
P2	'0C' = Keine FCI in der Antwort
Lc	'06' = Länge des zugehörigen Datenfeldes
Datenfeld	'D27600014400' = AID of DF.KT
Le	Nicht vorhanden

Tabelle 84 - (N3088.00) SELECT Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	'9000' oder spezifische Status-Bytes, siehe [HPC-P1]

5.11.4 Lesen der X.509-Zertifikate

Das Lesen der X.509-Zertifikate ist in Kapitel 10.4 von [HPC-P2] beschrieben.

5.11.5 Generierung einer Zufallszahl

Zur Generierung einer kryptographisch sicheren Zufallszahl wird das Kommando GET RANDOM gemäß Kapitel 14.9.7 von [HPC-P1] verwendet.

Tabelle 85 - (N3089.00) GET RANDOM Kommando zur Erzeugung einer sicheren Zufallszahl

CLA	Gemäß ISO/IEC 7816-4 für proprietäre Klasse
INS	'84' = GET RANDOM (identisch zu GET CHALLENGE)
P1, P2	'0000'
Lc	Nicht vorhanden
Datenfeld	Nicht vorhanden
Le	'xx' = Länge der erwarteten Zufallszahl in den Antwortdaten

Tabelle 86 - (N3090.00) GET RANDOM Antwort

Datenfeld	Zufallszahl
SW1-SW2	'9000' oder spezifische Status-Bytes; siehe [HPC-P1]

Die erzeugte Zufallszahl steht kartenintern nicht für weitere Aktionen zur Verfügung.

5.11.6 Verwendung des privaten Schlüssels

Der private Schlüssel PrK.SMKT.AUT kann ohne PIN-Eingabe verwendet werden. Zur Entschlüsselung eines verschlüsselten Geheimnisses muss der private Schlüssel und der Algorithmus mit dem ISO/IEC 7816-4-Kommando MSE ausgewählt werden.

Tabelle 87 - (N3091.00) MSE Kommando zur Schlüssel- und Algorithmenauswahl

CLA	Gemäß ISO/IEC 7816-4
INS	'22' = MANAGE SECURITY ENVIRONMENT
P1	'41' = SET für Entschlüsselung
P2	'B8' = Confidentiality Template
Lc	'06' = Länge des zugehörigen Datenfeldes
Datenfeld	'84 01 82' '80 01 81' = DO KeyRef von PrK.SMKT.AUT DO AlgID rsaDecipherPKCS1_V1_5
Le	Nicht vorhanden

Tabelle 88 - (N3092.00) MSE Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	'9000' oder spezifische Status-Bytes; siehe [HPC-P1]

Nachdem der Schlüssel und der Algorithmus gesetzt sind, kann die Entschlüsselungsoperation mit dem ISO/IEC 7816-8-Kommando PSO: DECIPHER ausgeführt werden.

Tabelle 89 – (N3093.00) PSO: DECIPHER Kommando

CLA	Gemäß ISO/IEC 7816-4
INS	'2A' = PERFORM SECURITY OPERATION: DECIPHER
P1	'80' = Rückgabe des Klartextes
P2	'86' = Verschlüsselte Daten im Datenfeld
Lc	'000101' = Länge des zugehörigen Datenfeldes = 257
Datenfeld	'00' (Padding indicator) Kryptogramm (256 bytes)
Le	'0000' oder '00xx' = Länge des entschlüsselten Geheimnisses

Tabelle 90 – (N3094.00) PSO: DECIPHER Antwort

Datenfeld	Entschlüsseltes Geheimnis
SW1-SW2	'9000' oder spezifische Status-Bytes; siehe [HPC-P1]

Zur Berechnung von Authentisierungsdaten wird das INTERNAL AUTHENTICATE Kommando verwendet. Bevor dieses Kommando ausgeführt werden kann, muss der private Schlüssel und der passende Algorithmus gesetzt werden.

Tabelle 91 – (N3095.00) MSE Kommando zur Schlüssel- und Algorithmenauswahl

CLA	Gemäß ISO/IEC 7816-4
INS	'22' = MANAGE SECURITY ENVIRONMENT
P1	'41' = SET für interne Authentisierung
P2	'A4' = Authentication Template
Lc	'06' = Länge des zugehörigen Datenfeldes
Datenfeld	'84 01 82' '80 01 02' = DO KeyRef von PrK.SMKT.AUT DO AlgID signPKCS1_V1_5
Le	Nicht vorhanden

Tabelle 92 - (N3096.00) MSE Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	'9000' oder spezifische Status-Bytes; siehe [HPC-P1]

Tabelle 93 - (N3097.00) INTERNAL AUTHENTICATE Kommando

CLA	Gemäß ISO/IEC 7816-4
INS	'88' = INTERNAL AUTHENTICATE
P1	'00'
P2	'00'
Lc	'00xxxx' = Länge des zugehörigen Datenfeldes
Datenfeld	Authentisierungsbezogene Daten; siehe Kapitel 14.7.4 in [HPC-P1]
Le	'0100' = Länge der erwarteten digitalen Signatur = 256

Tabelle 94 - (N3098.00) INTERNAL AUTHENTICATE Antwort

Datenfeld	Digitale Signatur
SW1-SW2	'9000' oder spezifische Status-Bytes; siehe [HPC-P1]

5.12 Laden einer neuen Anwendung oder Anlegen eines EFs nach Ausgabe der SMC-A

Es wird angenommen, dass das Laden neuer Anwendungen oder das Erstellen neuer EFs auf MF-Ebene (einschließlich Aktualisieren der Dateien EF.DIR und EF.Version) oder das Anlegen von neuen EFs in DF.SMA nach der Ausgabe der SMC-A von einem Card Application Management System (CAMS) durchgeführt wird. Dies ist ein optionaler Prozess.

Ebenso ist das CAMS optional. Die Inhalte des Kapitels 13 in [HPC-P2] sind allerdings normativ, wenn das Laden neuer Anwendungen oder das Erstellen neuer EFs nach Ausgabe der SMC-A durchgeführt werden müssen.

6 Sicherheitsmodulkarte B

6.1 ATR-Kodierung und technische Eigenschaften

Für die SMC-B gelten dieselben Konventionen für die technischen Eigenschaften, ATR und Übertragungsprotokolle wie für die HPC und die SMC-A, siehe Kapitel 11.2 in [HPC-P1] für die elektrische Schnittstelle und Kapitel 4.1 in [HPC-P2] für die ATR-Kodierung. Die SMC-B ist als Plug-In-Karte (ID-000) für die Nutzung in entsprechenden Kartenterminals vorgesehen.

6.2 Allgemeine Struktur

Die SMC-B enthält

- die Root-Anwendung (MF) mit einigen EFs auf MF-Ebene für allgemeine Datenobjekte, CV-Zertifikate, globale Schlüssel **und PIN** für Authentisierungsprozesse (z.B. Nachweis der Zugriffsberechtigung auf die eGK und Prüfen der Echtheit der eGK),
- die Sicherheitsmodulanwendung (DF.SMA) zur Bereitstellung von SMC-B-spezifischen Daten **und Dateien für Konfigurationsdaten des Konnektors und des Netzwerks,**
- die ESIGN-Anwendung (DF.ESIGN) mit PKI-Schlüsseln für die Organisationssignatur, Client/Server-Authentisierung, Entschlüsselung und Umschlüsselung von Dokumenten,
- die Kartenterminalanwendung (DF.KT) für die Authentisierung des Kartenterminals zum Verbindungsaufbau mit einem Konnektor.

Abbildung 5 (N3500.00) zeigt die prinzipielle Struktur der SMC-B.

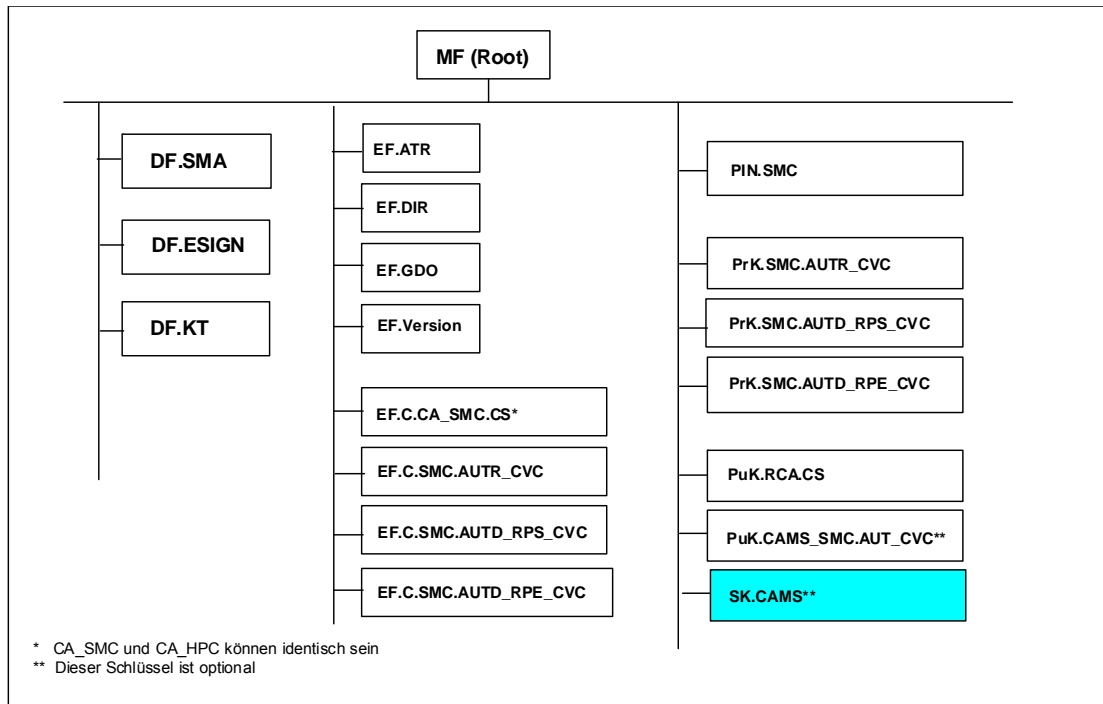


Abbildung 5 – (N3500.00) Allgemeine Struktur der SMC-B

Die Funktionalität der SMC-B umfasst die volle Funktionalität der SMC-A. Alle EFs der SMC-A sind auch in der SMC-B vorhanden. Zusätzlich sind in der SMC-B auf MF-Ebene ein weiteres CV-Zertifikat mit dem entsprechenden privaten Schlüssel für die funktionale Geräteauthentisierung und eine PIN verfügbar.

Außerdem steht in der SMC-B die ESIGN-Anwendung für PKI-Dienste zur Verfügung. Eine kryptografische Informationsanwendung (DF.CIA.ESIGN) ist nicht erforderlich, da eine SMC-B stationär gesteckt bleibt und die Anwendung der zuständigen Software bekannt ist.

6.3 Root-Anwendung und Dateien auf MF-Ebene

6.3.1 MF

Das MF der SMC-B ist ein "Application Dedicated File" (siehe Kapitel 8.3.1.3 in [HPC-P1]) mit den in Tabelle 95 (N3501.00) gezeigten Eigenschaften.

Tabelle 95 – (N3501.00) Attribute von MF

Attribut	Wert	Anmerkung
Objekttyp	Application Dedicated File	
Application Identifier	'D27600014606'	
File Identifier	'3F00'	Optional vorhanden
Life Cycle Status	Operational State (activated)	
Zugriffsregel in allen SEs		
Zugriffsart	Sicherheitsbedingung	Anmerkung
SELECT	ALWAYS	
LOAD APPLICATION (nach Ausgabe der SMC-B)	AUT('D27600014606' '01') AND SmMac AND SmCmdEnc	Nur ausführbar, wenn ein CAMS genutzt wird, siehe Kapitel 5.12. Falls ein CAMS mit symmetrischer Authentisierung eingesetzt wird, muss die Sicherheitsbedingung die Schlüsselreferenz des entsprechenden symmetrischen Schlüssels enthalten, d.h. AUT('13') statt

		AUT('D27600014600' '01')
ACTIVATE, DEACTIVATE, DELETE	NEVER	

6.3.2 EF.ATR

Eigenschaften und Nutzung von EF.ATR sind dieselben wie bei der SMC-A, siehe Kapitel 5.3.2.

6.3.3 EF.DIR

EF.DIR enthält die Anwendungs-Templates für MF, DF.SMA, DF.ESIGN und DF.KT gemäß ISO/IEC 7816-4. EF.DIR erlaubt den Eintrag von Anwendungskennungen weiterer (nachgeladener) Anwendungen, siehe folgende Tabelle mit den Eigenschaften von EF.DIR.

Tabelle 96 – (N3502.00) Attribute von MF / EF.DIR

Attribut	Wert	Anmerkung
Objektyp	Linear Variable Record Elementary File	
File Identifier	'2F00'	
Short File Identifier	'1E' = 30	
Number of Bytes	133	7 * max. Recordlänge
Maximum Number of Records	7 (3 für die zukünftige Verwendung)	
Maximum Record Length	19 Bytes	
Flag Record LCS	False	
Flag Transaction Mode	True	
Flag Checksum	True	
Life Cycle Status	Operational State (activated)	
Content	...	siehe Tabelle 97 (N3503.00)
Zugriffsregel in allen SEs		
Zugriffsart	Sicherheitsbedingung	Anmerkung
SELECT, READ RECORD, SEARCH RECORD	ALWAYS	
APPEND RECORD, UPDATE RECORD	AUT('D27600014600' '01') AND SmMac	Nur ausführbar, wenn ein CAMS genutzt wird, siehe Kapitel 5.12. Falls ein CAMS mit symmetrischer Authentisierung eingesetzt wird, muss die Sicherheitsbedingung die Schlüsselreferenz des entsprechenden symmetrischen Schlüssels enthalten, d.h. AUT('13') statt AUT('D27600014600' '01')
ACTIVATE, ACTIVATE RECORD, DEACTIVATE, DEACTIVATE RECORD, DELETE, ERASE RECORD	NEVER	

Die in EF.DIR enthaltenen Anwendungs-Templates sind in Tabelle 97 (N3503.00) gezeigt.

Tabelle 97 – (N3503.00) Anwendungs-Templates in EF.DIR der SMC-B

Tag	L	Anwendungs-Template	Bedeutung
'61'	'08'	'4F 06 D27600014606'	Anwendungs-Template mit AID.MF
'61'	'08'	'4F 06 D27600014607'	Anwendungs-Template mit AID.SMA
'61'	'0C'	'4F 0A A000000167 455349474E'	Anwendungs-Template mit AID.ESIGN
'61'	'08'	'4F 06 D27600014400'	Anwendungs-Template mit AID.KT

6.3.4 EF.GDO

Eigenschaften und Nutzung von EF.GDO sind dieselben wie bei der SMC-A, siehe Kapitel 5.3.4.

6.3.5 EF.Version

Eigenschaften und Nutzung von EF.Version sind dieselben wie bei der SMC-A, siehe Kapitel 5.3.5.

6.3.6 EF.C.CA_SMC.CS

Eigenschaften und Nutzung von EF.C.CA_SMC.CS und dem enthaltenen CV-Zertifikat sind dieselben wie bei der SMC-A, siehe Kapitel 5.3.6.

6.3.7 EF.C.SMC.AUTR_CVC

Eigenschaften und Nutzung von EF.C.SMC.AUTR_CVC und dem enthaltenen CV-Zertifikat sind dieselben wie bei der SMC-A, siehe Kapitel 5.3.7.

6.3.8 EF.C.SMC.AUTD_RPS_CVC

Eigenschaften und Nutzung von EF.C.SMC.AUTD_RPS_CVC und dem enthaltenen CV-Zertifikat sind dieselben wie bei der SMC-A, siehe Kapitel 5.3.8.

6.3.9 EF.C.SMC.AUTD_RPE_CVC

EF.C.SMC.AUTD_RPE_CVC enthält das CV-Zertifikat für die C2C-Geräteauthentisierung sowohl zwischen SMC-B/SMC-A, als auch zwischen SMC-B/SMC-B mit einer SMC-B als entfernter PIN-Empfänger. Die folgende Tabelle zeigt die Eigenschaften der Datei.

Tabelle 98 – (N3504.00) Attribute von MF / EF.C.SMC.AUTD_RPE_CVC

Attribut	Wert	Anmerkung
Objekttyp	Transparent Elementary File	
File Identifier	'2F05'	
Short File Identifier	'05' = 5	
Number of Bytes	341	
Flag Transaction Mode	False	
Flag Checksum	False	
Life Cycle Status	Operational State (activated)	
Content	...	siehe Tabelle (N2021.00) von [HPC-P2]
Zugriffsregel in allen SEs		
Zugriffsart	Sicherheitsbedingung	Anmerkung
SELECT, READ BINARY	ALWAYS	
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, UPDATE BINARY	NEVER	

Struktur und Inhalt des CV-Zertifikats in EF.C.SMC.AUTD_RPE_CVC mit CPI = '22' sind in Kapitel 7.1.3 von [HPC-P1] definiert und in [Tabelle \(N2021.00\)](#) von [HPC-P2] dargestellt. Die "Certificate Holder Authorization" für das Zertifikat C.SMC.AUTD_RPE_CVC zeigt die [Tabelle \(N2624.00\)](#) in Annex A.3 von [HPC-P2].

6.3.10 PIN.SMC

PIN.SMC ist die globale PIN der SMC-B, die genutzt wird für:

- die Autorisierung der SMC-B, welche mit der Zugriffsregel des privaten Authentisierungsschlüssels PrK.SMC.AUTR_CVC verbunden ist, siehe Tabelle 100 (N3506.00),
- die Aktualisierung der Sicherheitsmoduldaten in EF.SMD, siehe Tabelle 107 (N3514.00), und
- die PKI-Dienste der ESIGN Anwendung.

Die Nutzung eines 8-stelligen Rücksetzcodes (Personal Unblocking Key, PUK) wird durch einen Nutzungszähler beschränkt, dessen Anfangswert auf 10 gesetzt ist. Der Nutzungszähler wird bei jeder Nutzung heruntergezählt, unabhängig davon, ob der eingegebene Rücksetzcode richtig oder falsch ist. Die folgende Tabelle zeigt die Eigenschaften der PIN.

Tabelle 99 – (N3505.00) Attribute von MF / PIN.SMC

Attribut	Wert	Anmerkung
Objekttyp	Passwort	
Password Identifier	'01'	
Password Reference	'01'	
Secret	Wird personalisiert
Minimum Length	6	
Start Retry Counter	3	
Retry Counter	3	
Transport Status	Transport-PIN Zufallszahl oder Transport-PIN abgeleitet oder Transport-PIN fester Wert oder Reguläres Passwort	Wird personalisiert
Flag Enabled	True	
Start Security Status Evaluation Counter	Infinite	
PUK	...	Wird personalisiert
PUK Usage	10	
Zugriffsregel in allen SEs		
Zugriffsart	Sicherheitsbedingung	Anmerkung
CHANGE RD (Option '00')	ALWAYS	
GET PIN STATUS	ALWAYS	
RESET RC (Option '00' und '01')	ALWAYS	
VERIFY	ALWAYS	
Andere	NEVER	

Die Funktionen des PIN-Managements sind dieselben wie für die PIN.CH der HPC, siehe Kapitel 4.3.9 und Kapitel 4.6 in [HPC-P2].

6.3.11 PrK.SMC.AUTR_CVC

PrK.SMC.AUTR_CVC ist der globale private Schlüssel für die C2C-Authentisierung zwischen SMC/eGK. Die folgende Tabelle zeigt die Eigenschaften des privaten Authentisierungsschlüssels.

Tabelle 100 – (N3506.00) Attribute von MF / PrK.SMC.AUTR_CVC

Attribut	Wert	Anmerkung
Objekttyp	Privates RSA-Objekt	Profil 0 oder 2 oder 3 oder ...
Key Identifier	'10'	
Key Reference	'10'	
Private Key (2048 Bits)	Wird personalisiert
Algorithm Identifier	rsaRoleAuthentication rsaSessionkey4SM rsaSessionkey4TC	
Zugriffsregel in allen SEs		
Zugriffsart	Sicherheitsbedingung	Anmerkung
INTERNAL AUTHENTICATE	PWD(PIN.SMC) OR AUT('D27600004000' 'xx')	Authentisierung mit PIN.SMC oder Rollenauthentisierung einer HPC mit zugehörigem persönlichen Profil, z.B. Profil 2, siehe [HPC-P2], Tabelle (N2623.00) .
EXTERNAL AUTHENTICATE	ALWAYS	
Andere	NEVER	

Der öffentliche Schlüssel, der zu PrK.SMC.AUTR_CVC (mit Profil 2 oder 3 oder... des CVC-Inhabers), gehört, ist in [C.SMC.AUTR_CVC](#) enthalten.

6.3.12 PrK.SMC.AUTD_RPS_CVC

PrK.SMC.AUTD_RPS_CVC ist der globale private Schlüssel für die C2C-Authentisierung zwischen SMC/HPC, SMC/SMC oder SMC/RFID-Token in der Funktion des PIN-Senders. Die folgende Tabelle zeigt die Eigenschaften des privaten Authentisierungsschlüssels.

Tabelle 101 – (N3507.00) Attribute von MF / PrK.SMC.AUTD_RPS_CVC

Attribut	Wert	Anmerkung
Objekttyp	Privates RSA-Objekt	Profil 54 (PIN Sender)
Key Identifier	'12'	
Key Reference	'12'	
Private Key (2048 Bits)	Wird personalisiert
Algorithm Identifier	rsaSessionkey4TC rsaSessionkey4Intro	
Zugriffsregel in allen SEs		
Zugriffsart	Sicherheitsbedingung	Anmerkung
INTERNAL AUTHENTICATE	AUT('D27600004000' '35') OR AUT('D27600004000' '37')	Funktionale Geräteauthentisierung einer HPC (SSCD mit Profil 53), SMC oder RFID-Token (PIN-Empfänger mit Profil 55), siehe [HPC-P2], Tabelle (N2624.00) .
EXTERNAL AUTHENTICATE	ALWAYS	
Andere	NEVER	

Der öffentliche Schlüssel, der zu PrK.SMC.AUTD_RPS_CVC (mit Profil 54 des CVC-Inhabers) gehört, ist in [C.SMC.AUTD_RPS_CVC](#) enthalten.

6.3.13 PrK.SMC.AUTD_RPE_CVC

PrK.SMC.AUTD_RPE_CVC ist der globale private Schlüssel für die C2C-Authentisierung zwischen SMC/SMC in der Funktion des PIN-Empfängers. Die folgende Tabelle zeigt die Eigenschaften des privaten Authentisierungsschlüssels.

Tabelle 102 – (N3508.00) Attribute von MF / PrK.SMC.AUTD_RPE_CVC

Attribut	Wert	Anmerkung
Objekttyp	Privates RSA-Objekt	Profil 55 (PIN-Empfänger)
Key Identifier	'11'	
Key Reference	'11'	
Private Key	... (2048 Bits)	Wird personalisiert
Algorithm Identifier	rsaRoleAuthentication rsaSessionkey4SM rsaSessionkey4Intro	
Zugriffsregel in allen SEs		
Zugriffsart	Sicherheitsbedingung	Anmerkung
INTERNAL AUTHENTICATE	ALWAYS	
EXTERNAL AUTHENTICATE	ALWAYS	
Andere	NEVER	

Der öffentliche Schlüssel, der zu PrK.SMC.AUTD_RPE_CVC (mit Profil 55 des CVC-Inhabers) gehört, ist in C.SMC.AUTD_RPE_CVC enthalten.

6.3.14 PuK.RCA.CS

PuK.RCA.CS ist der öffentliche Schlüssel der Wurzel-CA. Eigenschaften und Nutzung des Schlüssels sind dieselben wie für die SMC-A, siehe Tabelle 20 (N3022.00) in Kapitel 5.3.11.

6.3.15 PuK.CAMS_SMC.AUT_CVC

PuK.CAMS_SMC.AUT_CVC (optional) ist der öffentliche Schlüssel des zur SMC-B gehörenden CAMS. Eigenschaften und Nutzung des Schlüssels sind dieselben wie für die SMC-A, siehe Tabelle 21 (N3023.00) in Kapitel 5.3.12.

6.3.16 SK.CAMS

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

Tabelle 103 – (N3509.00) Attribute von MF / SK.CAMS

Attribut	Wert	Anmerkung
Object type	3TDES Authentication Object	
Key Identifier	'13' = 19	
encKey	...	Wird personalisiert
macKey	...	Wird personalisiert
Algorithm Identifier	desSessionkey4SM	
Zugriffsregeln in allen SEs		
Zugriffsart	Zugriffsart	Anmerkung
MUTUAL AUTHENTICATE	PWD(PIN.SMC) OR AUT('D27600004000' 'xx')	Authentisierung mit PIN.SMC oder Rollenaauthentisierung einer HPC oder

		SMC mit zugehörigem persönlichen Profil, z.B. Profil 2; siehe [HPC-P2], Tabelle (N2623.00).
Other	NEVER	

6.4 Sicherheitsumgebungen auf MF-Ebene

Auf MF-Ebene wird ausschließlich das SE # 1 (Default-SE) verwendet. Es ist möglich, in SE # 1 einen Trusted Channel aufzubauen, um beispielsweise die PIN zum RFID-Token zu übertragen oder in zukünftigen Anwendungen Daten online zu bearbeiten.

6.5 Öffnen der SMC-B

6.5.1 Auswahl der Root-Anwendung

Nach dem Reset ist die Root-Anwendung automatisch ausgewählt. Zu einem späteren Zeitpunkt kann die Root-Anwendung beispielsweise durch ein SELECT Kommando mit Anwendungskennung selektiert werden, wie in Tabelle 104 (N3510.00) gezeigt ist.

Tabelle 104 - (N3510.00) SELECT Kommando zur MF-Auswahl

CLA	Gemäß ISO/IEC 7816-4
INS	'A4' = SELECT
P1	'04' = DF-Auswahl mittels AID
P2	'0C' = Keine FCI in der Antwort
Lc	'06' = Länge der AID im Datenfeld
Datenfeld	'D27600014606' = AID der Root-Anwendung (MF) of SMC-B
Le	Nicht vorhanden

Tabelle 105 - (N3511.00) SELECT Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	'9000' oder spezifische Status-Bytes, siehe [HPC-P1]

Anmerkung 1 – Der optionale FID '3F00' wird nicht für die MF-Auswahl verwendet, da nur im aktuellen Verzeichnis nach dem angegebenen FID gesucht wird, siehe Kapitel 14.2.6.10 von [HPC-P1].

6.5.2 Lesen EF.ATR und EF.GDO

Zum Lesen von EF.ATR und EF.GDO wird das READ BINARY Kommando verwendet, siehe Kapitel 4.5.3 in [HPC-P2]. Da die SMC-B im jeweiligen Kartenleser verbleibt, braucht dieses Kommando wahrscheinlich jeweils nur einmal ausgeführt zu werden.

6.5.3 Lesen EF.DIR und EF.Version

Zum Lesen von EF.DIR und EF.Version wird das READ RECORD Kommando verwendet, siehe Kapitel 4.5.4 in [HPC-P2]. Da die SMC-B im jeweiligen Kartenleser verbleibt, braucht dieses Kommando wahrscheinlich jeweils nur einmal ausgeführt zu werden.

6.5.4 Lesen der CV-Zertifikate der SMC-B

Zum Lesen der SMC-B-bezogenen CV-Zertifikate wird das READ BINARY Kommando verwendet, siehe Kapitel 4.5.5 in [HPC-P2]. Da die SMC-B im jeweiligen Kartenleser verbleibt, wird dieses Kommando wahrscheinlich jeweils nur einmal von der Softwareumgebung ausgeführt, in der die CV-Zertifikate z.B. zusammen mit der entsprechenden CHR der SMC-B gespeichert werden.

6.6 Management von Kanälen

Wie die SMC-A muss auch die SMC-B mindestens 4 logische Kanäle unterstützen, siehe Kapitel 11.4 in [HPC-P1]. Die maximale Anzahl logischer Kanäle wird in der Datei EF.ATR angezeigt, siehe Kapitel 5.3.2. Jeder Kanal besitzt seinen eigenen unabhängigen Sicherheitsstatus, d.h. eine externe Authentisierung der Rollenkennung in einem logischen Kanal setzt keinen Sicherheitszustand in irgendeinem anderen Kanal.

Die Verwaltung der logischen Kanäle erfolgt wie in Kapitel 5 von [HPC-P2] beschrieben.

6.7 Autorisierung der SMC-B

Die allgemeinen Aspekte des Autorisierungsprozesses aus Sicht der autorisierenden Karte sind in Kapitel 7.6 von [HPC-P2] beschrieben. Wie bei der SMC-A ist die Autorisierung der SMC-B technisch auf die Zugriffsregel des privaten Authentisierungsschlüssels PrK.SMC.AUTR_CVC abgebildet (siehe Tabelle 100 (N3506.00)), der in C2C-Authentisierungsprozessen eingesetzt wird.

Die Autorisierung kann durch externe Authentisierung einer HPC mit der passenden Rollenkennung in der CHA des entsprechenden CV-Zertifikats für Rollenauthentisierung (**C.HPC.AUTR_CVC**) erzielt werden; siehe **Tabelle (N2623.00)** des Annex A.3 in [HPC-P2]. Der Autorisierungsprozess, der in Kapitel 5.7 für the SMC-A beschrieben ist, findet auch für die SMC-B Anwendung.

Alternativ kann die SMC-B durch die erfolgreiche Präsentation der PIN.SMC autorisiert werden, siehe Kapitel 6.3.10.

6.8 Interaktionen zwischen SMC-B und eGK

Falls keine SMC-A verfügbar ist, z.B. in einer kleinen Institution, kann die SMC/eGK-Authentisierung mit oder ohne Aufbau eines Trusted Channel mit einer SMC-B anstelle der SMC-A erfolgen. Die in der Interaktion verwendeten Schlüssel und Algorithmen sind die gleichen wie in Kapitel 5.8 für die SMC-A beschrieben.

6.9 Interaktionen zwischen SMC-B und SMC-A oder RFID-Token

6.9.1 Allgemeines

Einen Überblick über mögliche Authentisierungsprozesse zwischen SMC/HPC, SMC/SMC und SMC/RFID-Token gibt das Kapitel 7.1 in [HPC-P2]. Die SMC-B unterstützt wie die SMC-A das GET SECURITY STATUS KEY Kommando, mit dem z.B. der Authentisierungsstatus einer vorgegebenen Rollenennung von der Karte abgerufen werden kann; siehe Kapitel 7.2 in [HPC-P2].

Die SMC-B in der Rolle des PIN-Senders nutzt den entsprechenden privaten Schlüssel für die Geräteauthentisierung, PrK.SMC.AUTD_RPS_CVC (Profil 54) für die Interaktion mit einem RFID-Token.

Die SMC-B in der Rolle des PIN-Empfängers nutzt den entsprechenden privaten Schlüssel für die Geräteauthentisierung, PrK.SMC.AUTD_RPE_CVC (Profil 55) für die Interaktion mit einer SMC-A, welche die Rolle des PIN-Senders einnimmt.

Vor dem asymmetrischen Authentisierungsprozess müssen die CV-Zertifikate der SMC-B gelesen werden, siehe Kapitel 5.5.4. Die CV-Zertifikate der Gegenseite müssen geprüft werden, so dass die entsprechenden öffentlichen Schlüssel in der SMC-B verfügbar sind.

6.9.2 Asymmetrische Authentisierung mit TC-Aufbau als PIN-Sender

Der private Schlüssel PrK.SMC.AUTD_RPS_CVC muss durch die externe Authentisierung der die PIN empfangenden Karte, d.h. eines RFID-Token, aktiviert werden. Das ist Teil des Authentisierungsprozesses, der wie in Kapitel 5.9.2 beschrieben abläuft. In der SMC-B wird dazu der Algorithmus RSA-Authentisierung mit Vereinbarung von Sitzungsschlüsseln für Trusted Channel gesetzt.

6.9.3 Asymmetrische Authentisierung mit Speicherung von Vorstellungsschlüsseln als PIN-Sender

Der private Schlüssel PrK.SMC.AUTD_RPS_CVC muss durch die externe Authentisierung der PIN empfangenden Karte, d.h. eines RFID-Token, aktiviert werden. Das ist Teil des Authentisierungsprozesses, der wie in Kapitel 5.9.3 beschrieben abläuft. In der SMC-B wird dazu der Algorithmus RSA-Authentisierung mit Vereinbarung von Vorstellungsschlüsseln gesetzt.

6.9.4 Asymmetrische Authentisierung mit TC-Aufbau als PIN-Empfänger

Der Authentisierungsprozess nutzt den privaten Schlüssel PrK.SMC.AUTD_RPE_CVC, wie in Kapitel 7.3 von [HPC-P2] beschrieben ist, wobei die SMC-B gegenüber der PIN sendenden Karte, d.h. einer SMC-A, die Stelle der HPC einnimmt. In der SMC-B wird dazu der Algorithmus RSA-Authentisierung mit Vereinbarung von Sitzungsschlüsseln für Secure Messaging gesetzt.

6.9.5 Asymmetrische Authentisierung mit Speicherung von Vorstellungsschlüsseln als PIN-Empfänger

Der Authentisierungsprozess nutzt den privaten Schlüssel PrK.SMC.AUTD_RPE_CVC, wie in Kapitel 7.4 von [HPC-P2] beschrieben ist, wobei die SMC-B gegenüber PIN sendenden Karte, d.h. einer SMC-A, die Stelle der HPC einnimmt. In der SMC-B wird dazu der Algorithmus RSA-Authentisierung mit Vereinbarung von Vorstellungsschlüsseln gesetzt.

6.9.6 Symmetrische Authentisierung als PIN-Sender

Falls eine bestimmte SMC-B und ein bestimmter RFID-Token sich bereits einander vorgestellt, d.h. eine asymmetrische Authentisierung mit persistenter Speicherung von Vorstellungsschlüsseln durchgeführt haben, können beide Karten unter Nutzung der gemeinsamen Vorstellungsschlüssel die symmetrische Authentisierung ausführen. Dieses Verfahren wird wie in Kapitel 5.9.4 beschrieben durchgeführt. In der SMC-B wird dazu der Algorithmus DES-Authentisierung mit Vereinbarung von Sitzungsschlüsseln für Trusted Channel ausgewählt.

6.9.7 Symmetrische Authentisierung als PIN-Empfänger

Falls eine bestimmte SMC-B und eine bestimmte SMC-A sich bereits einander vorgestellt, d.h. eine asymmetrische Authentisierung mit persistenter Speicherung von Vorstellungsschlüsseln durchgeführt haben, können beide Karten unter Nutzung der gemeinsamen Vorstellungsschlüssel die symmetrische Authentisierung ausführen. Dieses Verfahren wird wie in Kapitel 7.5 von [HPC-P2] beschrieben durchgeführt, wobei die SMC-B die Stelle der HPC einnimmt. In der SMC-B wird dazu der Algorithmus DES-Authentisierung mit Vereinbarung von Sitzungsschlüsseln für Secure Messaging ausgewählt.

6.10 Die Sicherheitsmodul-Anwendung

6.10.1 Dateistruktur und Dateiinhalt

Die folgende Abbildung zeigt die Dateistruktur von DF.SMA für die SMC-B.

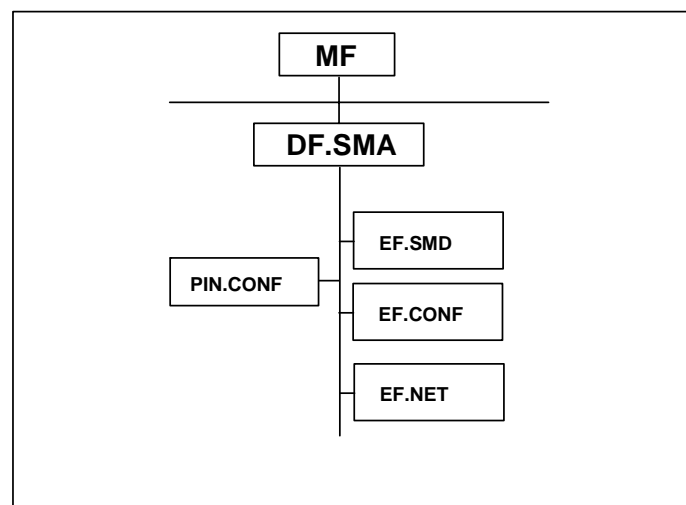


Abbildung 6 – (N3512.00) Prinzipielle Struktur der Sicherheitsmodul-Anwendung der SMC-B

6.10.2 DF.SMA (Security Module Application)

DF.SMA ist ein „Application Directory“ gemäß Kapitel 8.3.1.1 in [HPC-P1], d.h. ist mittels Anwendungskennung selektierbar. Tabelle 106 (N3513.00) zeigt die Eigenschaften des Anwendungsverzeichnisses.

Tabelle 106 – (N3513.00) Attribute von MF / DF.SMA

Attribut	Wert	Anmerkung
Objekttyp	Application Directory	
Application Identifier	'D27600014607'	
File Identifier	-	Herstellerspezifisch; Falls unterstützt, dann außerhalb des Intervalls ['1000', 'FEFF']; siehe Kapitel 8.1.1 in [HPC-P1]
Life Cycle Status	Operational State (activated)	
Zugriffsregel in allen SEs		
Zugriffsart	Sicherheitsbedingung	Anmerkung
SELECT	ALWAYS	
LOAD APPLICATION (nach Ausgabe der SMC-B)	AUT('D27600014600' '01') AND SmMac AND SmCmdEnc	Nur ausführbar, wenn ein CAMS genutzt wird, siehe 5.12. Falls ein CAMS mit symmetrischer Authentisierung eingesetzt wird, muss die Sicherheitsbedingung die Schlüsselreferenz des entsprechenden symmetrischen Schlüssels enthalten, d.h. AUT('13') statt AUT('D27600014600' '01')
ACTIVATE, DEACTIVATE, DELETE	NEVER	

6.10.2.1 EF.SMD

Die Nutzung der Datei EF.SMD ist dieselbe wie die für SMC-A, siehe Kapitel 5.10.1.2. Die in Tabelle 107 (N3514.00) definierten Zugriffsbedingungen unterscheiden sich jedoch leicht von denen in der SMC-A: Alternativ zur Authentisierung einer HPC oder einer SMC kann für den aktualisierenden oder löschenden Zugriff die Authentisierung mit der PIN.SMC genutzt werden.

Tabelle 107 – (N3514.00) Attribute von MF / DF.SMA / EF.SMD

Attribut	Wert	Anmerkung
Objekttyp	Transparent Elementary File	
File Identifier	'D001'	
Short File Identifier	'01' = 1	
Number of Bytes	1024	
Flag Transaction Mode	False	
Flag Checksum	True	
Life Cycle Status	Operational State (activated)	
Content	...	
Zugriffsregel in allen SEs		
Zugriffsart	Sicherheitsbedingung	Anmerkung
SELECT, READ BINARY	ALWAYS	
UPDATE BINARY, ERASE BINARY	PWD(PIN.SMC) OR AUT('D27600004000' 'xx')	Authentisierung mit PIN.SMC oder Rollenauthentisierung einer HPC oder einer SMC mit zugehörigem persönlichen Profil, z.B. Profil 2, siehe [HPC-P2], Tabelle (N2623.00) .
ACTIVATE, DEACTIVATE, DELETE	NEVER	

6.10.2.2 EF.CONF

Die transparente Datei EF.CONF speichert Konfigurationsdaten für die Konnektorwartung. Dies kann beispielsweise beim Austausch des Konnektors genutzt werden, um Pairing-Informationen zu sichern und an den neuen Konnektor zu übertragen. Lesen, Aktualisieren und Löschen der Daten sind nur nach erfolgreicher Präsentation der PIN.CONF zugelassen.

Die Zugriffsbedingungen und Eigenschaften von EF.CONF sind in der Tabelle 108 (N3515.00) definiert.

Tabelle 108 – (N3515.00) Attribute von MF / DF.SMA / EF.CONF

Attribut	Wert	Anmerkung
Objektyp	Transparent Elementary File	
File Identifier	'D002'	
Short File Identifier	'02' = 2	
Number of Bytes	8192	
Flag Transaction Mode	True	
Flag Checksum	True	
Life Cycle Status	Operational State (activated)	
Content	...	
Zugriffsregel in allen SEs		
Zugriffsart	Sicherheitsbedingung	Anmerkung
SELECT	ALWAYS	
READ BINARY, UPDATE BINARY, ERASE BINARY	PWD(PIN.CONF)	Authentisierung mit PIN.CONF, siehe Tabelle 110 (N3517.00)
ACTIVATE, DEACTIVATE, DELETE	NEVER	

6.10.2.3 EF.NET

Die transparente Datei EF.NET kann Netzwerkkonfigurationsdaten speichern, welche einen niedrigeren Schutzbedarf als die Daten in EF.CONF besitzen, z.B.

- DNS-Namen oder IP-Adressen in Verbindung mit Portnummer und Protokolltyp (TCP oder UDP) der Access Gateways,
- VPN IP-Version (IPv4 oder IPv6)
- DNS-Name des Aktualisierungsservers.

Die Daten sind organisationsspezifisch. Das Lesen der Daten ist immer möglich. Aktualisieren und Löschen ist nur nach erfolgreicher Präsentation der PIN.SMC zugelassen. Die Zugriffsbedingungen und weitere Eigenschaften der Datei EF.NET sind in Tabelle 109 (N3516.00) definiert.

Tabelle 109 – (N3516.00) Attribute von MF / DF.SMA / EF.NET

Attribut	Wert	Anmerkung
Objektyp	Transparent Elementary File	
File Identifier	'D003'	
Short File Identifier	'03' = 3	
Number of Bytes	2048	
Flag Transaction Mode	False	
Flag Checksum	True	
Life Cycle Status	Operational State (activated)	
Content	...	
Zugriffsregel in allen SEs		
Zugriffsart	Sicherheitsbedingung	Anmerkung
SELECT, READ BINARY	ALWAYS	
UPDATE BINARY, ERASE BINARY	PWD(PIN.SMC)	Die Zugriffsregel von PIN.SMC ist auf MF-Ebene definiert
ACTIVATE, DEACTIVATE, DELETE	NEVER	

6.10.2.4 PIN.CONF

PIN.CONF ist eine lokale PIN für den schreibenden und löschenden Zugriff auf Daten in EF.CONF. Die PIN besteht aus 6 bis 8 Ziffern und ist änderbar. Der Wiederholungszähler muss den Anfangswert 3 besitzen.

Die Nutzung eines 8-stelligen Rücksetzcodes (Personal Unblocking Key, PUK) wird durch einen Nutzungszähler beschränkt, dessen Anfangswert auf 10 gesetzt ist. Der Nutzungszähler wird bei jeder Nutzung heruntergezählt, unabhängig davon, ob der eingegebene Rücksetzcode richtig oder falsch ist. Die Eingabe des korrekten Wertes setzt den Wiederholungszähler von PIN.CONF auf den Anfangswert zurück. Der Sicherheitsstatus der PIN.CONF kann unbegrenzt verwendet werden, d.h. der Default-Wert von SSEC beträgt unendlich.

Die folgende Tabelle zeigt die Eigenschaften und Zugriffsregeln der PIN.CONF.

Tabelle 110 – (N3517.00) Attribute von MF / DF.SMA / PIN.CONF

Attribut	Wert	Anmerkung
Objekttyp	Passwort	
Password Identifier	'01'	
Password Reference	'81'	
Secret	Wird personalisiert
Minimum Length	6	
Start Retry Counter	3	
Retry Counter	3	
Transport Status	Einer der Verfahren in Kapitel 8.2.5 von [HPC-P1]	
Flag Enabled	True	
Start Security Status Evaluation Counter	Infinite	
PUK	...	Wird personalisiert
PUK Usage	10	
Zugriffsregel in allen SEs		
Zugriffsart	Sicherheitsbedingung	Anmerkung
CHANGE RD (Option '00')	ALWAYS	
GET PIN STATUS	ALWAYS	
RESET RC (Option '00' und '01')	ALWAYS	
VERIFY	ALWAYS	
Andere	NEVER	

Gemäß Kapitel 14.6.1.4 und 14.6.5.6 in [HPC-P1] prüft das COS ausschließlich die Minimallänge (6 Ziffern) von PIN.CONF, d.h. das COS kontrolliert nicht, ob die Maximallänge von 8 Ziffern überschritten wird.

Als PIN-Transportschutz muss ein Verfahren aus Kapitel 8.2.5 von [HPC-P1] verwendet werden. Es wird empfohlen, ein Leer-PIN Verfahren zu nutzen, bei dem der Benutzer nur die neue PIN eingeben muss. Zum Setzen der regulären PIN wird das Kommando CHANGE REFERENCE DATA verwendet, siehe Kapitel 4.6.2 in [HPC-P2].

Die Funktionen des PIN-Managements sind dieselben wie für die PIN.CH der HPC, siehe Kapitel 4.6 in [HPC-P2].

6.10.3 Auswahl der Anwendung

Die Auswahl der Anwendung wird mit dem ISO/IEC 7816-4 SELECT Kommando erzielt, wie in den folgenden zwei Tabellen gezeigt ist.

Tabelle 111 - (N3518.00) SELECT Kommando zur Auswahl von DF.SMA

CLA	Gemäß ISO/IEC 7816-4
INS	'A4' = SELECT
P1	'04' = DF-Auswahl mittels AID
P2	'0C' = Keine FCI in der Antwort
Lc	'06' = Länge des zugehörigen Datenfeldes
Datenfeld	'D27600014607' = AID von DF.SMA der SMC-B
Le	Nicht vorhanden

Tabelle 112 - (N3519.00) SELECT Antwort

Datenfeld	Nicht vorhanden
SW1-SW2	'9000' oder spezifische Status-Bytes, siehe [HPC-P1]

6.10.4 Lesen, Aktualisieren und Löschen von Daten in EF.SMD, EF.CONF und EF.NET

Zum Lesen, Aktualisieren und Löschen von Daten in EF.SMD, EF.CONF und EF.NET werden dieselben Kommandos wie in Kapitel 5.10.4 verwendet.

6.11 Die ESIGN-Anwendung

6.11.1 Dateistruktur und Dateiinhalt

DF.ESIGN wird verwendet für:

- die Berechnung einer Organisationssignatur (die Signatur ist an die entsprechende Institution im Gesundheitswesen gebunden, nicht an eine einzelne Person, siehe Abbildung 7 (N3520.00),
- die Client/Server-Authentisierung z.B. zur Verbindung der Institution im Gesundheitswesen oder eines Teils dieser Institution mit dem VPN des Gesundheitswesens und
- die Entschlüsselung und Umschlüsselung eines Dokumenten-Chiffrierungsschlüssels zur vertraulichen Weitergabe von Dokumenten, welche an die entsprechende Institution im Gesundheitswesen und nicht an eine einzelne Person adressiert sind.

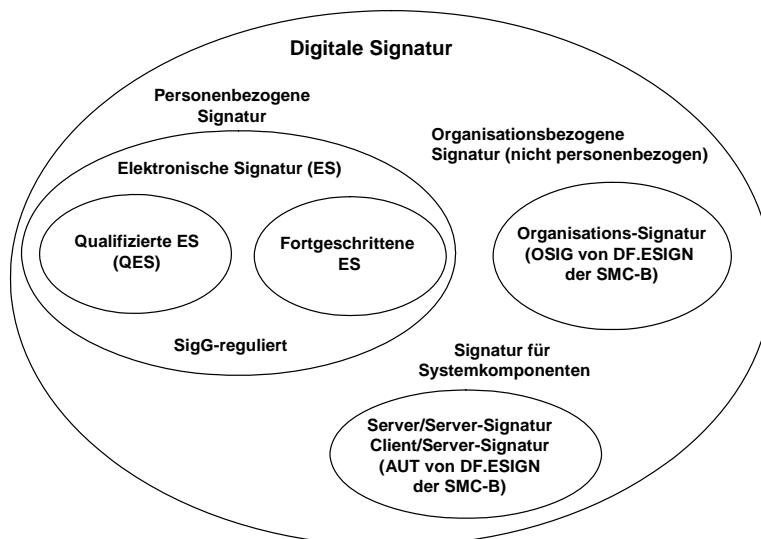


Abbildung 7 – (N3520.00) Arten der digitalen Signatur

Abbildung 8 (N3521.00) zeigt die prinzipielle Dateistruktur der ESIGN-Anwendung gemäß EN14890.

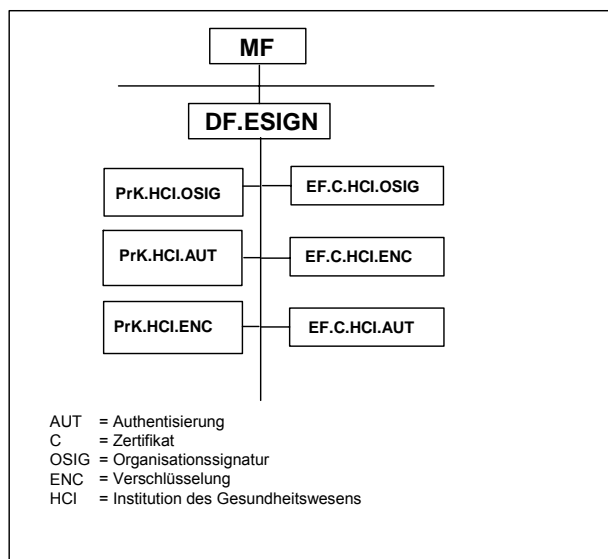


Abbildung 8 – (N3521.00) Allgemeine Struktur von DF.ESIGN

6.11.2 DF.ESIGN (ESIGN-Anwendung)

DF.ESIGN ist ein "Application Directory" gemäß Kapitel 8.3.1.1 in [HPC-P1], d.h. ist mittels Anwendungskennung auszuwählen. Tabelle 113 (N3522.00) zeigt die Eigenschaften des Anwendungsverzeichnisses.

Tabelle 113 – (N3522.00) Attribute von MF / DF.ESIGN

Attribut	Wert	Anmerkung
Objekttyp	Application Directory	
Application Identifier	'A000000167 455349474E'	
File Identifier	-	Herstellerspezifisch; Falls unterstützt, dann außerhalb des Intervalls ['1000', 'FEFF']; siehe Kapitel 8.1.1 in [HPC-

		P1]
Life Cycle Status	Operational State (activated)	
Zugriffsregel in allen SEs		
Zugriffsart	Sicherheitsbedingung	Anmerkung
SELECT	ALWAYS	
LOAD APPLICATION, ACTIVATE, DEACTIVATE, DELETE	NEVER	

6.11.3 EF.C.HCI.OSIG

EF.C.HCI.OSIG enthält das X.509-Zertifikat für die Funktion der Organisationssignatur der SMC-B. Tabelle 114 (N3523.00) zeigt die Eigenschaften der Zertifikatsdatei.

Tabelle 114 – (N3523.00) Attribute von MF / DF.ESIGN / EF.C.HCI.OSIG

Attribut	Wert	Anmerkung
Objektyp	Transparent Elementary File	
File Identifier	'C000'	
Short File Identifier	'10' = 16	
Number of Bytes	1536 oder auf Zertifikatslänge beschränkt	
Flag Transaction Mode	False	
Flag Checksum	False	
Life Cycle Status	Operational State (activated)	
Content	...	Wird personalisiert
Zugriffsregel in allen SEs		
Zugriffsart	Sicherheitsbedingung	Anmerkung
SELECT, READ BINARY	ALWAYS	
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, UPDATE BINARY	NEVER	

6.11.4 EF.C.HCI.AUT

EF.C.HCI.AUT enthält das X.509-Zertifikat für den Client/Server-Authentisierungsdienst der SMC-B. Tabelle 115 (N3524.00) zeigt die Eigenschaften der Zertifikatsdatei.

Tabelle 115 – (N3524.00) Attribute von MF / DF.ESIGN / EF.C.HCI.AUT

Attribut	Wert	Anmerkung
Objektyp	Transparent Elementary File	
File Identifier	'C500'	
Short File Identifier	'01' = 1	
Number of Bytes	1536 oder auf Zertifikatslänge beschränkt	
Flag Transaction Mode	False	
Flag Checksum	False	
Life Cycle Status	Operational State (activated)	
Content	...	Wird personalisiert
Zugriffsregel in allen SEs		
Zugriffsart	Sicherheitsbedingung	Anmerkung
SELECT, READ BINARY	ALWAYS	
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, UPDATE BINARY	NEVER	

6.11.5 EF.C.HCI.ENC

EF.C.HCI.ENC enthält das X.509-Zertifikat zum Entschlüsseln und Umschlüsseln von verschlüsselten Dokumenten, welche an die entsprechende Institution im Gesundheitswesen und nicht an eine einzelne Person adressiert sind. Tabelle 116 (N3525.00) zeigt die Eigenschaften der Zertifikatsdatei.

Tabelle 116 – (N3525.00) Attribute von MF / DF.ESIGN / EF.C.HCI.ENC

Attribut	Wert	Anmerkung
Objektyp	Transparent Elementary File	
File Identifier	'C200'	
Short File Identifier	'02' = 2	
Number of Bytes	1024 oder auf Zertifikatslänge beschränkt	
Flag Transaction Mode	False	
Flag Checksum	False	
Life Cycle Status	Operational State (activated)	
Content	...	Wird personalisiert
Zugriffsregel in allen SEs		
Zugriffsart	Sicherheitsbedingung	Anmerkung
SELECT, READ BINARY	ALWAYS	
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, UPDATE BINARY	NEVER	

6.11.6 PrK.HCI.OSIG

PrK.HCI.OSIG ist der private Schlüssel für den PKI-Dienst zur Berechnung einer Organisationssignatur. Die Eigenschaften des Schlüssels sind in der folgenden Tabelle dargestellt.

Tabelle 117 – (N3526.00) Attribute von MF / DF.ESIGN / PrK.HCI.OSIG

Attribut	Wert	Anmerkung
Objektyp	Privates RSA-Objekt	
Key Identifier	'04' = 4	
Key Reference	'84'	
Private Key (2048 Bits)	Wird personalisiert
Key Available	True	
Algorithm Identifier	signPKCS1_V1_5 signPSS sign9796_2_DS2	
Access Rule in SE # 1		
Zugriffsart	Sicherheitsbedingung	Anmerkung
COMPUTE DIGITAL SIGNATURE (P2 = '9E' oder 'AC')	PWD(PIN.SMC)	Die Zugriffsregel von PIN.SMC ist auf MF-Ebene definiert
Andere	NEVER	

Die Länge des Schlüssels entspricht der für qualifizierte elektronische Signaturen bis Ende 2013 empfohlenen Schlüssellänge [TR-03116].

6.11.7 PrK.HCI.AUT

PrK.HCI.AUT ist der private Schlüssel für den PKI-Dienst zur Client/Server-Authentisierung. Die Eigenschaften des Schlüssels sind in der folgenden Tabelle dargestellt.

Tabelle 118 – (N3527.00) Attribute von MF / DF.ESIGN / PrK.HCI.AUT

Attribut	Wert	Anmerkung
Objekttyp	Privates RSA-Objekt	
Key Identifier	'02' = 2	
Key Reference	'82'	
Private Key (2048 Bits)	Wird personalisiert
Key Available	True	
Algorithm Identifier	INTERNAL AUTHENTICATE: rsaClientAuthentication PSO: COMPUTE DIGITAL SIGNATURE: signPKCS1_V1_5 signPSS sign9796_2_DS2	
Zugriffsregel in allen SEs		
Zugriffsart	Sicherheitsbedingung	Anmerkung
INTERNAL AUTHENTICATE, COMPUTE DIGITAL SIGNATURE (P2 = '9E' oder 'AC')	PWD(PIN.SMC)	Die Zugriffsregel von PIN.SMC ist auf MF- Ebene definiert
Andere	NEVER	

Die Länge des Schlüssels entspricht der für Client/Server-Authentierung bis Ende 2013 empfohlenen Schlüssellänge [TR-03116].

6.11.8 PrK.HCI.ENC

PrK.HCI.ENC ist der private Schlüssel für den PKI-Dienst zur Entschlüsselung und Umschlüsselung eines Dokumenten-Chiffrierungsschlüssels. Die Eigenschaften des Schlüssels sind in der folgenden Tabelle dargestellt.

Tabelle 119 – (N3528.00) Attribute von MF / DF.ESIGN / PrK.HCI.ENC

Attribut	Wert	Anmerkung
Objekttyp	Privates RSA-Objekt	
Key Identifier	'03' = 3	
Key Reference	'83'	
Private Key (2048 Bits)	Wird personalisiert
Key Available	True	
Algorithm Identifier	rsaDecipherOaep rsaDecipherPKCS1_V1_5	
Zugriffsregel in allen SEs		
Zugriffsart	Sicherheitsbedingung	Anmerkung
PSO: DECIPHER, PSO: TRANSCIPHER	PWD(PIN.SMC)	Die Zugriffsregel von PIN.SMC ist auf MF- Ebene definiert
Andere	NEVER	

Die Länge des Schlüssels entspricht der für Verschlüsselung bis Ende 2013 empfohlenen Schlüssellänge [TR-03116].

6.11.9 Lesen der X.509-Zertifikate

Das Lesen der X.509-Zertifikate ist in Kapitel 10.4 von [HPC-P2] beschrieben.

6.11.10 Nutzen der privaten Schlüssel

Bevor einer der privaten Schlüssel genutzt werden kann, muss die PIN.SMC erfolgreich eingegeben werden.

Zur Berechnung einer elektronischen Signatur mit dem PSO: COMPUTE DIGITAL SIGNATURE Kommando wird die in Kapitel 9.8 von [HPC-P2] beschriebene Kommandosequenz verwendet.

Die Client-Server-Authentisierung wird gemäß Kapitel 10.6 in [HPC-P2] durchgeführt.

Das Entschlüsseln eines Dokumenten-Chiffrierungsschlüssels mit dem PSO: DECIPHER Kommando ist in Kapitel 10.7 von [HPC-P2] beschrieben.

Das Umschlüsseln eines Dokumenten-Chiffrierungsschlüssels erfolgt mit dem in Kapitel 10.8 von [HPC-P2] beschriebenen Kommando PSO: TRANSCIPHER.

6.12 Die Kartenterminal-Anwendung

Eigenschaften und Nutzung von DF.KT sind dieselben wie für die SMC-A, siehe Kapitel 5.11.

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

Es wird angenommen, dass das Laden neuer Anwendungen oder das Erstellen neuer EFs auf MF-Ebene (einschließlich Aktualisieren der Dateien EF.DIR und EF.Version) oder das Anlegen von neuen EFs in DF.SMA nach der Ausgabe der SMC-B von einem Card Application Management System (CAMS) durchgeführt wird. Dies ist ein optionaler Prozess.

Ebenso ist das CAMS optional. Die Inhalte des Kapitels 13 in [HPC-P2] sind allerdings normativ, wenn das Laden neuer Anwendungen oder das Erstellen neuer EFs nach Ausgabe der SMC-B durchgeführt werden müssen.