Specification

German
Health Professional Card
and
Security Module Card

Part 3: SMC Applications and Functions

Version 2.3.2

05.08.2009

Bundesärztekammer

Kassenärztliche Bundesvereinigung

Bundeszahnärztekammer

Bundespsychotherapeutenkammer

Kassenzahnärztliche Bundesvereinigung

Bundesapothekerkammer

Deutsche Krankenhausgesellschaft

Editor: Ulrich Waldmann (Fraunhofer-Institut SIT)

The HPC specification consists of the following parts:

Part 1: Commands, Algorithms and Functions of the COS Platform
Part 2: HPC Applications and Functions
Part 3: SMC Applications and Functions

Revision History

Date	Version	Modifications
21.09.2005	SMC V2.09	New version based on HPC-P1 (V0.8) and HPC-P2 (V2.09)
07.10.2005	SMC V2.09	Changes: - Update of Table A.2a
19.11.2005	SMC V2.1 Draft	Changes: - Addition of EF.ATR, EF.SMD and EF.NET - Addition of CVC.SMC.TCE - Indication of TC support method in EF.ATR - Completion and update of access rules - Authentication procedures with global Keys moved to MF level - Simplification of interaction HPC/SMC (only asym. Authentication) - Reduction of public keys to the Root CA PuK
14.12.2005	SMC V2.1	Changes: - Harmonization CVC with eGK - DF.ASIG integrated in DF.ESIGN
21.02.2006	SMC V2.1.0	Changes: - Harmonization with eGK - Clarification of SMC signature type
18.05.2007	SMC V2.1.1	Changes: - Addition of SMC authorization with PIN.SMC - Addition of PrK.SMC.AUT activation by external authentication of an HPC or SMC - Addition of profile 7: paramedic - Completion and update of access rules - Addition of PrK.SMC.AUT activation for C2C authentication between HPC and SMC - Error and editorial corrections - Precisions Protection Profile for SMC must be updated because of the security relevant PIN-activation
04.07.2008	SMC V2.2.0 – V2.3.0	Changes: - Adjustments for interoperability with the eGK generation 1 - Changes in respect to stack and comfort signatures - Adjustments of algorithms, key lengths etc. to BSI technical guidelines
09.04.2009	V2.3.1	SRQ-0009 "HPC-P3 Corrigenda 1" SRQ-0014 "Introductionkeys in HBA und SMC" SRQ-0015 "Inhalt von EF.Version"
05.08.2009	V2.3.2	SRQ-0016 "Introductionkeys und Sicherheitszustand" SRQ-0017 "Festlegungen zum CAMS-Schlüssel" SRQ-0019 "HPC-P3 Corrigenda 2"

Contents

1 Scope

This part of the specification defines the card interface to

- the Security Module Cards SMC-A and SMC-B designed for use in health institutions.

SMC-A and SMC-B provide services such as

- C2C authentication SMC/eGK
- trusted channel support, i.e. computation, decipherment, and verification of secure messaging objects as remote PIN sender, allowing secure PIN transfer to a PIN receiving card (HPC, RFID Token or SMC-B). It may also be used in future applications for secured transfer of other data.
- support of authentication of card terminal towards connector.

SMC-B provides additional services such as

- organizational signatures for the related health care institution
- client/server authentication for the related health care institution
- encipherment service for the related health care institution, so that enciphered documents can be deciphered by the authorized personal of the related health care institution
- trusted channel support as remote PIN receiver executing secure messaging commands
- support of connector maintenance by storage of related configuration data.

The SMCs are used in card terminals of the health institutions.

2 References

[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; see www.bundesnetzagentur.de

[COM-PKI-1]
T7, TeleTrusT: Common PKI Specification, Part 1: Certificate and CRL Profiles, Version 2.0,
20th 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/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: Spezifikation der elektronischen Gesundheitskarte
Teil 1: Spezifikation der elektrischen Schnittstelle
Version 2.2.2, 16.09.2008

[eGK-P2]
gematik: 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]
prEN 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]
German Health Professional Card and Security Module Card

Part 1: Commands, Algorithms and Functions of the COS Platform
Version 2.3.2, 05.08.2009

[HPC-P2]
German Health Professional Card and Security Module Card
Part 2: HPC Applications and Functions
Version 2.3.2, 05.08.2009

[ISO3166]
ISO/IEC 3166-1: 2006
Codes for the representations of names of countries and their subdivisions – Part 1: Country codes

[ISO7812]
ISO/IEC 7812-1: 2006
Identification cards – 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 of 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]
ISO9796-2: 2002, Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms

[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: 1994
Information technology - digital compression and coding of continuous-tone still images: Requirements and guidelines

[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 v2.1: RSA Cryptography Standard
June 14, 2002 (earlier versions: V1.5: Nov. 1993, V2.0: July, 1998)

[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-CC-PP-0018-V2-2009, Version 2.5, April 6th, 2009

[PP-SMC-A]
BSI: Common Criteria Protection Profile – Secure Module Card Type A (PP-SMC-A), BSI-PP-0019, Version 1.9.1, February 1st, 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 1st, 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/IEC 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]
Law Governing Framework Conditions for Electronic Signatures and Amending Other Regulations (Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften), Bundesgesetzblatt Nr. 22, 2001, S.876

[SigV01]
Ordinance on Electronic Signatures (Verordnung zur elektronischen Signatur – SigV), 2001, Bundesgesetzblatt 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 Abbreviations and Notations

3.1 Abbreviations

AC	Attribute Certificate
AID	Application Identifier
AKS	Auslöser KomfortSignatur (Comfort Signature Trigger)
AOD	Authentication Object Directory
APDU	Application Protocol Data Unit [ISO7816-3]
ASN.1	Abstract Syntax Notation One
ASCII	American Standard Code for Information Interchange
ATR	Answer-to-Reset
AUT	Authentication
AUTD	CV-based device-authentication
AUTR	CV-based role-authentication
AUTO	Organization-specific Authentication
BA	Berufsausweis (professional card)
BCD	Binary Coded Decimal
BER	Basic Encoding Rules
BNA	Bundesnetzagentur (Federal Network Agengy)
C	Certificate
C2C	Card-to-Card
CA	Certification Authority
CAMS	Card Application Management System
CAR	Certification Authority Reference
CC	Cryptographic Checksum
CD	Certificate Directory
CER	Canonical Encoding Rules
CG	Cryptogram
CH	Cardholder
CHA	Certificate Holder Authorization
CHR	Certificate Holder Reference
CIA	Cryptographic Information Application
CIO	Cryptographic Information Objects
CLA	Class-Byte of a command APDU
COS	Card Operating System
CPI	Certificate Profile Identifier
CRL	Cerificate Revocation List

CS	CertSign (CertificateSigning)
CTA	Card Terminal Application
CV	Card Verifiable
CVC	Card Verifiable Certificate
D,DIR	Directory
DE	Data Element
DER	Distinguished Encoding Rules
DES	Daten Encryption Standard
DF	Dedicated File
DI	Baud rate adjustment factor
DM	Display Message
DO	Data Objekt
DS	Digital Signature
DSI	Digital Signature Input
DTBS	Data to be signed
ECDSA	Elliptic Curve Digital Signature Algorithm
EF	Elementary File
eGK	elektronische Gesundheitskarte (electronic Health Card) [eGK-P1] and [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 (compulsory health insurance)
GP	Global Platform
HB	Historical Bytes
HBA	Heilberufsausweis (Health Professional Card)
HCI	Health Care Institution
HP	Health Professional
HPA	Health Professional Application
HPC	Health Professional Card
HPD	Health Professional related Data
ICC	Integrated Circuit Card
ICCSN	ICC Serial Number

ICM	IC Manufacturer
ID	Identifier
IFSC	Information Field Size Card
IIN	Issuer Identification Number
INS	Instruction-Byte of a command APDU
KeyRef	Key Reference
KM	Komfortmerkmal (comfort feature)
KT	Karten-Terminal (card terminal)
LCS	Life Cicle Status
LSB	Least Significant Byte(s)
MAC	Message Authentication Code
MF	Master File
MII	Major Industry Identifier
MSE	Manage Security Environment
OCSP	Online Certicate Status Protocol
OD	Object Directory
OID	Object Identifier
OSIG	Organisation Signature
PIN	Personal Identification Number
PIX	Proprietary Application Provider Extension
PK,PuK	Public Key
PKCS	Public Key Cryptography Standard (here [PKCS#1])
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure for X.509 Certificates (IETF)
PP	Protection Profile
PrK	Private Key
PSO	Perform Security Operation
PUK	Personal Unblocking Key (Resetting Code)
PV	Plain Value
P1	Parameter P1 of a command APDU
P2	Parameter P2 of a command APDU
QES	Qualified Electronic Signature
RA	Registration Authority
RAM	Random Access Memory
RC	Retry Counter
RCA	Root CA
RD	Reference Data
RF	Radio Frequency

RFC	Request für Comment
RFID	Radio Frequency Identification
RFU	Reserved for future use
RID	Registered Application Provider Identifier
RND	Random Number
ROM	Read Only Memory
RPE	Remote PIN-Receiver
RPS	Remote PIN-Sender
RSA	Algorithmus of Rivest, Shamir, Adleman [RSA]
SAK	Signaturanwendungskomponente (signature creation component)
SE	Security Environment
SFID	Short EF Identifier
SIG	Signature
SigG	Signaturgesetz (Signature Law) [SigG01]
SigV	Signaturverordnung (Signature Ordinance) [SigV01]
SK	Secret Key
SM	Secure Messaging
SMA	Security Module Application
SMC	Security Module Card
SMD	Security Module Data
SMKT	Sicherheitsmodul Kartenterminal (Security Module Card Terminal)
SN	Serial Number
SO	Security Officer (administrator)
SSCD	Secure Signature Creation Device
SSEC	Security Status Evaluation Counter
SSEE	Sichere Signaturerstellungseinheit (secure signature creation device)
SSL	Security Sockets Layer [SSL]
SUK	Stapel- und Komfortsignatur (stack and comfort signature)
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 (Certification Authority)
3TDES	3-Key-Triple-DES

3.2 Notations

For keys and certificates the following simplified Backus-Naur notation applies (see [PKI-Nota] for definitions):

<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>

For subsequent data items the following notation is used:

|| = Concatenation of data

For simplification X.509v3 certificates are addressed without version number.

4 Security Module Card Types

An SMC provides similar functions as an HPC, but the X.509 certificates - if used - are not related to a single person but to a health care institution HCI or a related organizational entity (e.g. doctor practice, pharmacy, a hospital or a part of it).

The following SMC types have to be distinguished:

Table 1 – (N3001.00) SMC Types

SMC Type	Functionality	Use Cases
SMC-A used e.g. in card terminals (referred as "Arbeitsplatzkarte")	Asymmetric CVC authentication procedure without establishment of a trusted channel	SMC-A authorization, Access to eGK after SMC-A authorization
	Asymmetric CVC authentication procedure with establishment of a trusted channel	SMC-A as PIN sender: secured PIN transfer to an HPC, SMC-B or RFID Token
	Trusted channel support, i.e. PSO operations COMPUTE CC, ENCIPHER, DECIPHER, VERIFY CC, and (optionally) ENVELOPE command to process secure messaging data objects	SMC-A as PIN sender: secured PIN transfer to an HPC, SMC-B or RFID Token
	Persistent storage of session keys (introduction keys) to enable a more efficient symmetric C2C authentication	SMC-A as PIN sender: secured PIN transfer to an HPC, SMC-B or RFID Token
	Symmetric CVC authentication procedure with establishment of a trusted channel	SMC-A as PIN sender: secured PIN transfer to an HPC, SMC-B or RFID Token
	KT-Application (DF.KT) to support authentication of card terminal	Authentication of card terminal towards connector by using the authentication key stored in the SMC-A
SMC-B used e.g. as single per organizational entity in a card terminal (referred as "Institutionenkarte")	Functionality of SMC-A	Use cases of SMC-A
	PIN.SMC for HP authentication	SMC-B authorization
	Secure messaging support, i.e. processing secure messaging commands	SMC-B as PIN receiver: secured reception of PIN.SMC
	PKI keys for OSIG, ENC & AUT and related X.509 certificates (no attribute certificates)	PKI services for the respective Health Care Institution (HCI): - Deciphering and transciphering of enciphered documents addressed to the HCI and not to a single person - Client/server authentication - Organizational signature function
	EF.CONF for connector configuration data	Provision of configuration data for connector maintenance purposes (high security level)
	EF.NET for network configuration data	Provision of network configuration data (of lower security level)

5 Security Module Card A

5.1 ATR coding and Technical Characteristics

For the SMC-A the same conventions apply for the technical characteristics, Answer-to-Reset and transmission protocols as for the HPC. See Chapter 11.2 of [HPC-P1] for the electrical interface and Clause 4.1 of [HPC-P2] for ATR coding. The SMC-A is designed for use as plug-in card (ID-000) present in related card terminals.

5.2 General Structure

The SMC-A contains

- the Root Application (MF) with some EFs at MF level for general data objects, CV certificates and global keys for authentication procedures (e.g. proving access rights to the eGK and verification of the authenticity of the eGK),
- the Security Module Application (DF.SMA) for the provision of SMC-A related data file(s),
- the Card Terminal Application (DF.KT) for authentication of the card terminal to connect to a specific connector.

The general structure of SMC-A is shown in Figure 1 (N3002.00).

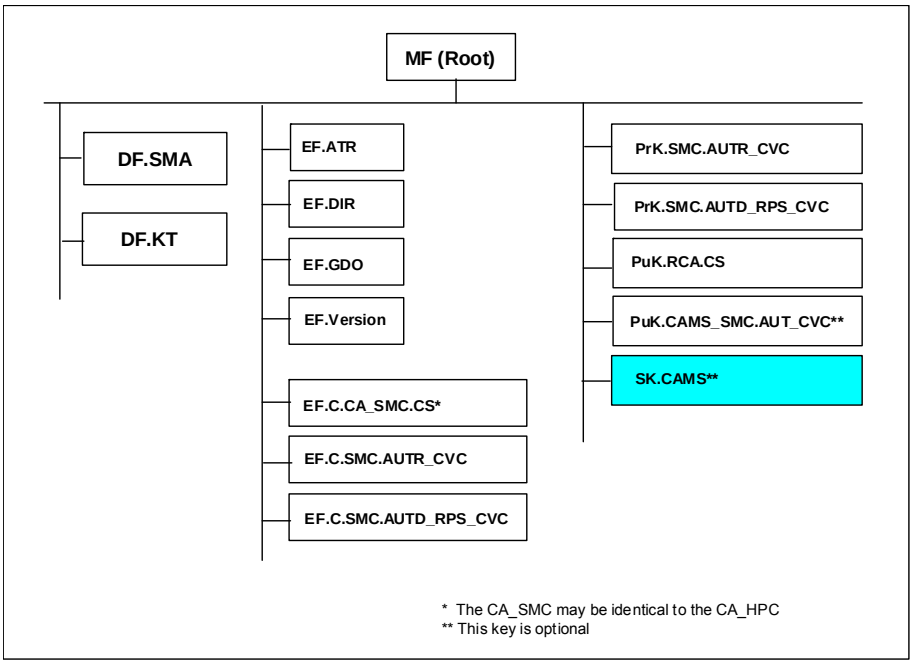

Figure 1 – (N3002.00) General file structure of an SMC-A

5.3 Root Application and Elementary Files at MF-Level

5.3.1 MF

The MF of SMC-A is an Application Dedicated File (see Clause 8.3.1.3 of [HPC-P1]) and has got the characteristics shown in Table 2 (N3003.00).

Table 2 – (N3003.00) Characteristics of MF

Attribute	**Value**	**Note**
Object type	Application Dedicated File	
Application Identifier	‘D27600014604’	
File Identifier	‘3F00’	Optional
Life Cycle Status	Operational state (activated)	
Access Rule in all SEs		
Access Mode	**Security Condition**	**Note**
SELECT	ALWAYS	
LOAD APPLICATION (after SMC-A issuing)	AUT(‘D27600014600' || '01’) AND SmMac AND SmCmdEnc	Only executable if a CAMS is used; see Clause 5.12. If a CAMS with symmetric authentication is used, then the security condition must contain the key reference of the corresponding symmetric key, i.e. AUT('13') instead of AUT(‘D27600014600' || '01’).
ACTIVATE, DEACTIVATE, DELETE	NEVER	

5.3.2 EF.ATR

The transparent file EF.ATR contains a constructed data object for indication of I/O buffer sizes and the DO 'Pre-issuing data' relevant for CAMS services. The characteristics of EF.ATR are shown in the following table.

Table 3 – (N3004.00) Characteristics of MF / EF.ATR

Attribute	**Value**	**Note**
Object type	Transparent Elementary File	
File Identifier	‘2F01’	Acc. to [ISO7816-4]
Short File Identifier	‘1D’ = 29	
Number of Bytes	COS specific	
Flag Transaction Mode	False	
Flag Checksum	True	
Life Cycle Status	Operational state (activated)	
Content	...	see Table 4 (N3005.00)
Access Rule in all SEs		
Access Mode	**Security Condition**	**Note**
SELECT, READ BINARY	ALWAYS	
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, UPDATE BINARY	NEVER	

The content of EF.ATR is specified in the subsequent tables.

Table 4 – (N3005.00) Content of EF.ATR

Tag	L	Value	Meaning
'E0'	'xx'	'02 xx xxxx 02 xx xxxx 02 xx xxxx 02 xx xxxx'	DO I/O buffer sizes; see Table 5 (N3006.00)
'66'	'xx'	'46 xx …' see Table 6 (N3007.00) || '47 04 x6 21 Dx xx'; see Table 7 (N3008.00) and Table 8 (N3009.00)	DO Card Data: DO Pre-issuing data || DO Card Capabilities with 4th byte = TC support method

The data object I/O buffer sizes shown in Table 5 (N3006.00) has 4 embedded DOs (Tag '02' = Integer value, length field 1 Byte with value '02' or '03', value field = max. number of bytes of the respective APDU).

Table 5 – (N3006.00) Data object input/output buffer size

Tag	Length	Value
'E0'	'xx'	'02' -L-'xxxx' || '02' -L-'xxxx' || '02'-L-'xxxx' || '02'-L-'xxxx' = - DO max. length of command APDU without SM || - DO max. length of response APDU without SM || - DO max. length of command APDU with SM || - DO max. length of response APDU with SM

NOTE – In contrast to the Note 1 in Clause 11.5.5 of [HPC-P1] and Note 1 in Clause 11.5.6 of [HPC-P1] it is not possible to specify maximum length values, which depend on specific combinations of CLA, INS, P1 and P2. This may be defined in later versions of this document when appropriate data structures are admitted in [ISO7816-4].

Table 6 – (N3007.00) Value of DO Pre-issuing Data (Tag '46')

L (byte)	Meaning of concatenated data elements (most significant byte: ICM)
1	IC manufacturer ID (see www.sc17.com)
5	Card manufacturer ID (see DIN-RA: http://sit.sit.fraunhofer.de/_karten_ident/SIT/rid_sde)
x	IC-ID (card manufacturer specific)
x	COS version (card manufacturer specific)
x	ROM mask (card manufacturer specific)

Table 7 – (N3008.00) Value of DO Card Capabilities (Tag '47')

b8	b7	b6	b5	b4	b3	b2	b1	**Meaning of 1st byte ('x6')**
1	-	-	-	-	-	-	-	DF selection by full DF name
-	x	-	-	-	-	-	-	DF selection by partial DF name (not determined)
-	-	x	-	-	-	-	-	DF selection by path (not determined)
-	-	-	1	-	-	-	-	DF selection by file identifier
-	-	-	-	0	-	-	-	Implicit DF selection (not supported)
-	-	-	-	-	1	-	-	Short EF identifier supported
-	-	-	-	-	-	1	-	Record number supported
-	-	-	-	-	-	-	0	Record identifier (not supported)
b8	b7	b6	b5	b4	b3	b2	b1	**Meaning of 2nd byte ('21')**
0	-	-	-	-	-	-	-	EFs of TLV structure (not supported)
-	0	1	-	-	-	-	-	Behavior of write functions (proprietary)
-	-	-	0	-	-	-	-	Value 'FF' for the first byte of BER-TLV tag fields invalid
-	-	-	-	0	0	0	1	Data unit size in quartets (power of 2, i.e. '01' = 2 quartets = one byte)
b8	b7	b6	b5	b4	b3	b2	b1	**Meaning of 3rd byte ('Dx')**
1	-	-	-	-	-	-	-	Command chaining supported; see Note 1
-	1	-	-	-	-	-	-	Extended Lc and Le fields
-	-	0	-	-	-	-	-	b6 is RFU (b6 = 0 recommended)
-	-	-	1	0	-	-	-	Logical channel number assignment by the card
					y	z	t	
-	-	-	-	-	x	x	x	Maximum number of logical channels; see Note 2

NOTE 1 – Command Chaining may be required for the LOAD APPLICATION command; see Clause 5.12.

NOTE 2 – The card capability bytes are set according to Clause 8.1.1.2.7 of [ISO7816-4]. In the 3rd capabilities byte the bits b3-b1 encode the maximum number of logical channels supported by the card: y, z, t not all set to 1 means 4y+2z+t+1, i.e. from one to seven, y = z = t = 1 means eight or more. The maximum number of supported logical channels shall be set to one of the following values: b3b2b1 = 011 (4 channels), 100 (5 channels), 101 (6 channels), 110 (7 channels) or 111 (≥ 8 channels).

Table 8 – (N3009.00) Value of the 4th card capabilities byte: TC support method

b8	b7	b6	b5	b4	b3	b2	b1	**Meaning**
x	x	x	x	x	x	0	0	No information given
						0	1	PSO
						1	1	PSO and ENVELOPE

5.3.3 EF.DIR

EF.DIR contains the application template for MF, DF.SMA, and DF.KT according to ISO/IEC 7816-4. EF.DIR allows the addition of AIDs of further (downloaded) applications. See the following table for characteristics of EF.DIR.

Table 9 – (N3010.00) Characteristics of MF / EF.DIR

Attribute	**Value**	**Note**
Object type	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 for future use)	
Maximum Record Length	19 bytes	
Flag Record LCS	False	
Flag Transaction Mode	True	
Flag Checksum	True	
Life Cycle Status	Operational state (activated)	
Content	...	see Table 10 (N3011.00)
Access Rule in all SEs		
Access Mode	**Security Condition**	**Note**
SELECT, READ RECORD, SEARCH RECORD	ALWAYS	
APPEND RECORD, UPDATE RECORD	AUT(‘D27600014600' || '01’) AND SmMac	Only executable if a CAMS is used; see Clause 5.12. If a CAMS with symmetric authentication is used, then the security condition must contain the key reference of the corresponding symmetric key, i.e. AUT('13') instead of AUT(‘D27600014600' || '01’).
ACTIVATE, ACTIVATE RECORD, DEACTIVATE, DEACTIVATE RECORD, DELETE, ERASE RECORD	NEVER	

The application templates contained in EF.DIR are shown in Table 10 (N3011.00).

Table 10 – (N3011.00) Application Templates in EF.DIR of SMC-A

Tag	**L**	**Application Template**	**Meaning**
’61’	‘08’	‘4F 06 D27600014604’	Application Template with AID.MF
’61’	‘08’	‘4F 06 D27600014605’	Application Template with AID.SMA
‘61’	‘08’	‘4F 06 D27600014400’	Application Template with AID.KT

5.3.4 EF.GDO

Table 11 (N3012.00) shows the attributes of EF.GDO.

Table 11 – (N3012.00) Characteristics of MF / EF.GDO

Attribute	Value	Note
Object type	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	...	see Table 12 (N3013.00)
Access Rule in all SEs		
Access Mode	**Security Condition**	**Note**
SELECT, READ BINARY	ALWAYS	
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, UPDATE BINARY	NEVER	

EF.GDO contains in compliance with [Resolution190] the DO ICC Serial Number; see Table 12 (N3013.00).

Table 12 – (N3013.00) ICC Serial No. for health cards

Tag	L	Value	Meaning
'5A'	'0A'	'80276 …'	ICCSN

The structure of the DO ICCSN (Tag '5A') for health cards is shown in Figure 2 (N3014.00).

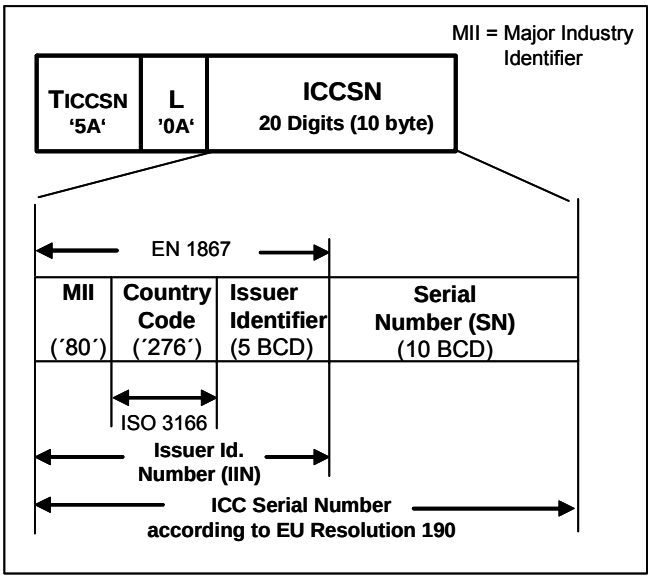

Figure 2 - (N3014.00) ICC Serial No. for health cards

Only a registered IIN is allowed as part of the ICCSN; see Annex A.1 of [HPC-P2].

It is the responsibility of the card issuer to ensure that the serial number (SN) is unique (especially in the case that several card manufacturers are involved). For this purpose, the two leading BCDs of the serial number (following the issuer identifier) indicate the engaged CA; see Annex A.2 of [HPC-P2].

5.3.5 EF.Version

The EF.Version with linear fixed record structure contains the version numbers of the specification parts and an SRQ number – indicating the upper limit of relevant SRQs – which the card is compliant to. The characteristics of the file EF.Version are shown in the subsequent table.

Table 13 – (N3015.00) Characteristics of MF / EF.Version

Attribute	**Value**	**Note**
Object type	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	...	see Table 14 (N3016.00).
Access Rule in all SEs		
Access Mode	**Security Condition**	**Note**
SELECT, READ RECORD, SEARCH RECORD	ALWAYS	
UPDATE RECORD	AUT('D27600014600' || '01') AND SmMac	Only executable if a CAMS is used; see Clause 5.12. If a CAMS with symmetric authentication is used, then the security condition must contain the key reference of the corresponding symmetric key, i.e. AUT('13') instead of AUT('D27600014600' || '01').
ACTIVATE, ACTIVATE RECORD, APPEND RECORD, DEACTIVATE, DEACTIVATE RECORD, DELETE, ERASE RECORD	NEVER	

The file EF.Version contains 4 records of fixed length; see Table 14 (N3016.00). The first 3 records indicate the 3 parts of the HPC specification and an SRQ number related to the card. The triplet version number XX.YY.ZZ of the respective specification part together with the four-digit SRQ number SSSS is encoded as XXYYZZSSSS in BCDs. The last record is reserved for future use (RFU).

Table 14 – (N3016.00) Content of EF.Version

Rec No.	Value (5 Bytes)	Meaning
1	'0203020000'	Version of supported HPC Specification Part 1 followed by the upper SRQ number limit, which the card is compliant to. In this case version 2.3.2, no additional SRQ
2	'0203020000'	Version of supported HPC Specification Part 2 followed by the upper SRQ number limit, which the card is compliant to. In this case version 2.3.2, no additional SRQ
3	'0203020000'	Version of supported HPC Specification Part 3 followed by the upper SRQ number limit, which the card is compliant to. In this case version 2.3.2, no additional SRQ
4	'0000000000'	RFU

5.3.6 EF.C.CA_SMC.CS

EF.C.CA_SMC.CS contains the card verifiable certificate of the Certificate Service Provider, issued by the Root CA for Health Care for a CA_SMC. The CA_SMC is possibly the same as the CA_HPC. All CV certificates of an HPC or SMC are derived from the same CV Root Certification Authority. The file characteristics of EF.C.CA_SMC.CS are outlined in Table 15 (N3017.00).

Table 15 – (N3017.00) Characteristics of MF / EF.C.CA_SMC.CS

Attribute	Value	Note
Object type	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	...	see [HPC-P2], Table (N2019.00)
Access Rule in all SEs		
Access Mode	**Security Condition**	**Note**
SELECT, READ BINARY	ALWAYS	
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, UPDATE BINARY	NEVER	

The coding of the CV certificates for a CA and the contained OID are described in Clause 4.3.6 of [HPC-P2]. The structure and content of the CVC in EF.C.CA_SMC.CS with CPI = '21' are defined in Clause 7.1 of [HPC-P1] and outlined in Table (N2019.00) of [HPC-P2].

5.3.7 EF.C.SMC.AUTR_CVC

EF.C.SMC.AUTR_CVC contains the card verifiable certificate of the SMC-A for role-based card-to-card authentications between eGK/SMC and authorization procedures between HPC/SMC and SMC/SMC. The characteristics of the file are shown in the following table.

Table 16 – (N3018.00) Characteristics of MF / EF.C.SMC.AUTR_CVC

Attribute	Value	Note
Object type	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	...	see [HPC-P2], Table (N2021.00)
Access Rule in all SEs		
Access Mode	**Security Condition**	**Note**
SELECT, READ BINARY	ALWAYS	
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, UPDATE BINARY	NEVER	

The coding of the CV certificates for an SMC-A and the contained OID are described in Clause 4.3.6 and Clause 4.3.7 of [HPC-P2]. The structure and content of the CVC in EF.C.SMC.AUTR_CVC with CPI = '22' are defined in Clause 7.1 of [HPC-P1] and outlined in Table (N2021.00) of [HPC-P2].

The Certificate Holder Authorizations relevant for a C.SMC.AUTR_CVC and other CV certificates of the health card family are shown in Table (N2623.00) of Annex A.3 of [HPC-P2].

5.3.8 EF.C.SMC.AUTD_RPS_CVC

EF.C.SMC.AUTD_RPS_CVC contains the card verifiable certificate of the SMC-A for card-to-card authentications between devices, in order to remotely send an entered PIN to the HPC, SMC-B or RFID Token; see Note. This certificate can be used without PIN authentication.

NOTE – Both the presentation of RFID Token and the PIN entry for the RFID Token takes place locally, probably at the same authentication terminal, but uses the remote PIN transfer modus to protect data at the air interface.

Table 17 – (N3019.00) Characteristics of MF / EF.C.SMC.AUTD_RPS_CVC

Attribute	**Value**	**Note**
Object type	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	...	see [HPC-P2], Table (N2021.00)
Access Rule in all SEs		
Access Mode	**Security Condition**	**Note**
SELECT, READ BINARY	ALWAYS	
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, UPDATE BINARY	NEVER	

The coding of the CV certificates for an SMC-A and the contained OID are described in Clause 4.3.6 and 4.3.7 of [HPC-P2]. The structure and content of the CVC in EF.C.SMC.AUTD_RPS_CVC with CPI = '22' are defined in Clause 7.1 of [HPC-P1] and outlined in Table (N2021.00) of [HPC-P2].

The Certificate Holder Authorizations relevant for a C.SMC.AUTD_RPS_CVC are shown in Table (N2624.00) of Annex A.3 of [HPC-P2].

5.3.9 PrK.SMC.AUTR_CVC

PrK.SMC.AUTR_CVC is the global private key for C2C-authentication between SMC/eGK. The use of the private key must be authorized by a health professional of a related profile, i.e. by external authentication of an HPC or SMC (see Clause 5.7) with an appropriate role ID of the card holding person/organization; see Table (N2623.00) in Annex A.3 of [HPC-P2]. The key characteristics are shown in Table 18 (N3020.00).

Table 18 – (N3020.00) Characteristics of MF / PrK.SMC.AUTR_CVC

Attribute	Value	Note
Object type	Private RSA Object	Profile 2 or 3 or ...
Key Identifier	'10'	
Key Reference	'10'	
Private Key	.... (2048 bit)	To be personalized
Algorithm Identifier	rsaRoleAuthentication, rsaSessionkey4SM rsaSessionkey4TC	
Access Rule in all SEs		
Access Mode	**Security Condition**	**Note**
INTERNAL AUTHENTICATE	AUT('D27600004000' || 'xx')	Role authentication of HPC or SMC with related personal profile, e.g. profile 2; see [HPC-P2], Table (N2623.00).
EXTERNAL AUTHENTICATE	ALWAYS	
Other	NEVER	

The public key associated with PrK.SMC.AUTR_CVC (of CVC holder profile 2 or 3 or...) is contained in the file C.SMC.AUTR_CVC.

5.3.10 PrK.SMC.AUTD_RPS_CVC

PrK.SMC.AUTD_RPS_CVC is the global private key for C2C-authentication between SMC/HPC, SMC/SMC, or SMC/RFID Token for PIN transfer to the PIN receiving card (HPC, SMC-B, RFID Token). The use of the private key requires the external authentication of a card with PIN receiving functionality (profile 53 of HPC or profile 55 of SMC-B and RFID Token; see Table (N2624.00) in Annex A.3 of [HPC-P2]). The key characteristics are shown in Table 19 (N3021.00).

Table 19 – (N3021.00) Characteristics of MF / PrK.SMC.AUTD_RPS_CVC

Attribute	Value	Note
Object type	Private RSA Object	Profile 54 (PIN Sender)
Key Identifier	'12'	
Key Reference	'12'	
Private Key	.... (2048 bit)	To be personalized
Algorithm Identifier	rsaSessionkey4TC rsaSessionkey4Intro	
Access Rule in all SEs		
Access Mode	**Security Condition**	**Note**
INTERNAL AUTHENTICATE	AUT('D27600004000' || '35') OR AUT('D27600004000' || '37')	Device authentication of HPC (SSCD with profile 53) or SMC or RFID Token (Remote PIN receiver with profile 55); see [HPC-P2], Table (N2624.00)
EXTERNAL AUTHENTICATE	ALWAYS	
Other	NEVER	

The public key associated with PrK.SMC.AUTD_RPS_CVC (of CVC holder profile 54) is contained in the file C.SMC.AUTD_RPS_CVC.

5.3.11 PuK.RCA.CS

PuK.RCA.CS is the public key of the Root CA for verification of CVCs issued by this RCA. The subsequent table shows the characteristics of the public key.

Table 20 – (N3022.00) Characteristics of MF / PuK.RCA.CS

Attribute	Value	Note
Object type	Public RSA Signature Verification Object	
Key Identifier	CAR of C.CA_SMC.CS: CA name (5 bytes) || extension (3 byte)	To be personalized
Key Reference	-	
Public Key	.... (2048 bit)	To be personalized
OID	´2B240304020204´ = {1 3 36 3 4 2 2 4}	
Access Rule in all SEs		
Access Mode	**Security Condition**	**Note**
VERIFY CERTIFICATE	ALWAYS	
Other	NEVER	

5.3.12 PuK.CAMS_SMC.AUT_CVC

PuK.CAMS_SMC.AUT_CVC (optional) is the public key for performing an asymmetric SMC/CAMS authentication procedure with TC establishment. The subsequent table shows the characteristics of the public key.

Table 21 – (N3023.00) Characteristics of MF / PuK.CAMS_SMC.AUT_CVC

Attribute	Value	Note
Object type	Public RSA Authentication Object	
Key Identifier	'000000000000000000000013' (12 byte)	To be personalized
CHA	'D2760001460001'	
Public Key	.... (2048 bit)	To be personalized
OID	'2B2403050204' = {1 3 36 3 5 2 4}	
Algorithm Identifier	rsaSessionkey4SM	
Access Rule in all SEs		
Access Mode	**Security Condition**	**Note**
INTERNAL AUTHENTICATE	ALWAYS	
EXTERNAL AUTHENTICATE	ALWAYS	
Other	NEVER	

5.3.13 SK.CAMS

SK.CAMS (optional) is the secret key for performing an SMC-A / CAMS authentication procedure with TC establishment. The subsequent table shows the characteristics of the key.

Table 22 – (N3024.00) Characteristics of MF / SK.CAMS

Attribute	Value	Note
Object type	3TDES Authentication Object	
Key Identifier	'13' = 19	
encKey	...	To be personalized
macKey	...	To be personalized
Algorithm Identifier	desSessionkey4SM	
Access Rule in all SEs		
Access Mode	**Security Condition**	**Note**
MUTUAL AUTHENTICATE	AUT('D27600004000' || 'xx')	Role authentication of HPC or SMC with related personal profile, e.g. profile 2; see [HPC-P2], Table (N2623.00).
Other	NEVER	

5.4 Security Environments at MF Level

At MF level only SE # 1 (default SE) is used. It is possible in SE # 1 to establish a trusted channel, e.g. for remote PIN transfer to the HPC, SMC-B or RFID Token or for online data processing in future applications.

5.5 SMC-A Opening

5.5.1 Selecting the Root Application

After reset the root application is selected by default. Afterwards, the root application can be selected, e.g. by using the SELECT command with application identifier as shown in Table 23 (N3025.00).

Table 23 - (N3025.00) SELECT command for MF selection

CLA	As defined in ISO/IEC 7816-4
INS	‘A4’ = SELECT
P1	‘04’ = DF selection by AID
P2	‘0C’ = No FCI to return
Lc	‘06’ = Length of AID in the data field
Data field	‘D27600014604’ = AID of Root Application (MF) of SMC-A
Le	Absent

Table 24 - (N3026.00) SELECT response

Data field	Absent
SW1-SW2	‘9000’ or specific status bytes; see [HPC-P1]

NOTE – The optional FID ‘3F00’ is not used for MF selection since only the current directory is searched for the file identifier; see Clause 14.2.6.10 of [HPC-P1].

5.5.2 Reading EF.ATR and EF.GDO

For reading EF.ATR and EF.GDO, the READ BINARY command is used; see Clause 4.5.3 of [HPC-P2]. Since the SMC-A remains in the respective device, this command is possibly performed only once.

5.5.3 Reading EF.DIR and EF.Version

For reading EF.DIR and EF.Version, the READ RECORD command is used; see Clause 4.5.4 of [HPC-P2]. Since the SMC-A remains in the respective device, this command is possibly performed only once.

5.5.4 Reading SMC-A related CV Certificates

For reading SMC-A related CV Certificates, the READ BINARY command is used; see Clause 4.5.5 of [HPC-P2]. Since the SMC-A remains in the respective device, this command is possibly performed only once by the software environment, which stores the CVCs e.g. associated with the respective CHR of the SMC-A.

5.6 Channel Management

The SMC-A shall support at least 4 logical channels; see Clause 11.4 of [HPC-P1]. The maximum number of logical channels is indicated in EF.ATR; see 5.3.2. Each channel has its own independent security status, i.e. the external authentication of a role identifier in one channel does not set a security status in any other channel.

The channel management shall be performed as specified in Chapter 5 of [HPC-P2].

5.7 Authorization of the SMC-A

The general aspects of the authorization process from the perspective of the authorizing card are outlined in Clause 7.6 of [HPC-P2]. The authorization of the SMC-A is technically mapped to the access rule of PrK.SMC.AUTR_CVC (see Table 18 (N3020.00)) which is used in card-to-card authentication procedures. This Clause describes the commands required on the side of the SMC-A to be authorized.

The authorization is achieved by an external HPC or SMC authentication with the appropriate role ID present in the CHA of the respective card verifiable certificate for role authentication (C.HPC. AUTR_CVC of an HPC or C.SMC.AUTR_CVC of an SMC); see Table (N2623.00) in Annex A.3 of [HPC-P2].

Prior to the authentication procedure the CV certificates of the counterpart have to be verified by the SMC-A to import the public key PuK.HPC.AUTR_CVC or PuK.SMC.AUTR_CVC.

The authentication procedure to be performed corresponds to the second part (HPC authentication) of the authentication procedure between eGK and HPC described in Clause 6.4 of [HPC-P2].

In a first step of the external authentication of the authorizing card, the public key for role authentication of the authorizing card together with the appropriate algorithm have to be set.

Table 25 - (N3027.00) MSE command for key and algorithm selection

CLA	As defined in ISO/IEC 7816-4
INS	‘22’ = MANAGE SECURITY ENVIRONMENT
P1	‘81’ = SET for external authentication
P2	‘A4’ = Authentication Template in data field
Lc	‘11’ = Length of subsequent data field
Data field	‘83 0C xx ... xx’ || ‘80 01 00’ = DO KeyRef of PuK.HPC.AUTR_CVC or PuK.SMC.AUTR_CVC || DO AlgID rsaRoleCheck
Le	Absent

NOTE – The CHR of the CV certificate of the counterpart is taken as key reference. It has a length of 12 bytes: index set to '00' (1 byte) || KeyRef of PrK.HPC.AUTR_CVC or PrK.SMC.AUTR_CVC (1 byte) || ICCSN of the counterpart, i.e. ICCSN.HPC or ICCSN.SMC; see Clause 8.5.2 of [HPC-P1] for CHR structure.

Table 26 - (N3028.00) MSE response

Data field	Absent
SW1-SW2	‘9000’ or specific status bytes; see [HPC-P1]

Then, a challenge is requested from the SMC-A.

Table 27 - (N3029.00) GET CHALLENGE command

CLA	As defined in ISO/IEC 7816-4
INS	'84' = GET CHALLENGE
P1, P2	'0000'
Lc	Absent
Data field	Absent
Le	'08'

Table 28 - (N3030.00) GET CHALLENGE response

Data field	RND.SMC (8 byte)
SW1-SW2	'9000' or specific status bytes; see [HPC-P1]

The challenge is presented to the authorizing card together with the 8 LSB of SMC-A's ICCSN. Before the INTERNAL AUTHENTICATE can be performed by the authorizing card, the security status for the usage of the private key (PrK.HPC.AUTR_CVC or PrK.SMC.AUTR_CVC) has to be set by an appropriate authentication, i.e. in the HPC by a user authentication with PIN.CH and in the SMC-B by a user authentication with PIN.SMC or by an external authentication with a related role identifier. The resulting digital signature of the INTERNAL AUTHENTICATE is presented to the SMC-A in the EXTERNAL AUTHENTICATE command.

Table 29 – (N3031.00) EXTERNAL AUTHENTICATE command for authentication of HPC or SMC

CLA	As defined in ISO/IEC 7816-4
INS	'82' = EXTERNAL AUTHENTICATE
P1	'00' = Algorithm already known to the card
P2	'00' = Key reference already known to the card
Lc	'000100' = Length of subsequent data field = 256
Data field	Authentication related data; see Clause 14.7.1 of [HPC-P1]
Le	Absent

Table 30 – (N3032.00) EXTERNAL AUTHENTICATE response

Data field	Absent
SW1-SW2	'9000' or specific status bytes; see [HPC-P1]

The authentication related data produced by the authorizing card will be verified by the SMC-A, which sets – if authentication successful – the security status required for the usage of the PrK.SMC.AUTR_ CVC. This private key is used, e.g. for SMC/eGK interactions.

5.8 Interactions between SMC-A and eGK

5.8.1 Asymmetric SMC/eGK Authentication without TC Establishment

The SMC/eGK authentication is performed in the same way as the HPC/eGK authentication; see Clause 6.4 of [HPC-P2] with the SMC-A on behalf of the HPC. For this purpose, the private authentication key for role authentication PrK.SMC.AUTR_CVC is used.

5.8.2 Asymmetric SMC/eGK Authentication with TC Establishment

If future applications are intended for remotely processing eGK data, a trusted channel between an eGK and an SMC-A has to be established. The commands at the SMC-A interface after CVC verification are the same as for SMC/eGK authentication without TC establishment except for setting different algorithm identifiers.

The algorithm RSA authentication with agreement on session keys for secure messaging has to be set on side of the eGK. On side of the SMC-A the RSA authentication with agreement on session keys for trusted channel is the corresponding algorithm to be set.

5.9 Interactions between SMC-A and HPC or SMC-B or RFID Token

5.9.1 General

An overview about the possible authentication procedures between SMC/HPC, SMC/SMC and SMC/ RFID Token is given in Clause 7.1 of [HPC-P2]. The SMC-A also supports the GET SECURITY STATUS KEY command for querying e.g. the authentication status of a specified role identifier; see Clause 7.2 of [HPC-P2].

The SMC-A as remote PIN sender uses the corresponding private authentication key for device authentication, PrK.SMC.AUTD_RPS_CVC, to interact with an HPC, SMC-B or RFID Token. Before the asymmetric authentication procedure can be performed, the CVCs of the SMC-A must have been read; see Clause 5.5.4. The CV certificates related to the involved target card (HPC, SMC-B or RFID Token) are to be verified, so that the corresponding public keys will be available in the SMC-A.

Since the private key PrK.SMC.AUTD_RPS_CVC of the SMC-A for sending a remote PIN must be activated by external authentication of a related HPC, SMC-B or RFID Token (which receives a remote PIN) the respective PIN receiver will be authenticated first. The RSA authentication with agreement on session keys for trusted channel or storage of introduction keys are the algorithms to be set in the SMC-A.

5.9.2 Asymmetric Authentication with TC Establishment

In the first part of the procedure the HPC proves its authenticity to the SMC-A activating the private key PrK.SMC.AUTD_RPS_CVC. Before the command for external authentication is sent to the SMC-A, the key reference for the public authentication key of the target card and the appropriate algorithm identifier must be set.

Table 31 - (N3033.00) MSE command for key and algorithm selection

CLA	As defined in ISO/IEC 7816-4
INS	‘22’ = MANAGE SECURITY ENVIRONMENT
P1	‘81’ = SET for external authentication
P2	‘A4’ = Authentication Template in data field
Lc	‘11’ = Length of subsequent data field
Data field	‘83 0C xx ... xx’ || ‘80 01 74’ = DO KeyRef of PuK.HPC.AUTD_SUK_CVC (HPC) or PuK.SMC.AUTD_RPE_CVC (SMC-B) or PuK.KM.AUTD_RPE_CVC (RFID Token); see Note || DO AlgID rsaSessionkey4TC
Le	Absent

NOTE – The CHR of the counterpart’s CV certificate is used as key reference. It has a length of 12 byte: index set to '00' (1 byte) || KeyRef of private key of counterpart (1 byte) || ICCSN of counterpart (10 byte); see Clause 8.5.2 of [HPC-P1] for CHR structure.

Table 32 - (N3034.00) MSE response

Data field	Absent
SW1-SW2	‘9000’ or specific status bytes; see [HPC-P1]

Furthermore, the key reference for PrK.SMC.AUTD_RPS_CVC and the appropriate algorithm identifier are set for internal authentication.

Table 33 - (N3035.00) MSE command for key and algorithm selection

CLA	As defined in ISO/IEC 7816-4
INS	‘22’ = MANAGE SECURITY ENVIRONMENT
P1	‘41’ = SET for internal authentication
P2	‘A4’ = Authentication Template in data field
Lc	‘06’ = Length of subsequent data field
Data field	’84 01 10’ || ‘80 01 74' = DO KeyRef of PrK.SMC.AUTD_RPS_CVC || DO AlgID rsaSessionkey4TC
Le	Absent

Table 34 - (N3036.00) MSE response

Data field	Absent
SW1-SW2	‘9000’ or specific status bytes; see [HPC-P1]

NOTE – Both MSE SET commands for external and internal authentication are performed successively, so that the sequence of authentication commands will not be interrupted by a MSE SET command; see Chapter 15 of [HPC-P1].

Then, the external software will request a challenge from the SMC-A.

Table 35 - (N3037.00) GET CHALLENGE command

CLA	As defined in ISO/IEC 7816-4
INS	‘84’ = GET CHALLENGE
P1, P2	‘0000’
Lc	Absent
Data field	Absent
Le	‘08’

Table 36 - (N3038.00) GET CHALLENGE response

Data field	RND.SMC (8 bytes)
SW1-SW2	‘9000’ or specific status bytes; see [HPC-P1]

The challenge is presented to the counterpart (HPC, SMC-B or RFID Token) together with the 8 LSB of SMC's ICC Serial number. The resulting digital signature of the INTERNAL AUTHENTICATE performed by the counterpart is presented to the SMC-A in the EXTERNAL AUTHENTICATE command. The SMC-A has to verify the signature of the counterpart.

Table 37 – (N3039.00) EXTERNAL AUTHENTICATE command for authentication of the counterpart

CLA	As defined in ISO/IEC 7816-4
INS	'82' = EXTERNAL AUTHENTICATE
P1	'00' = Algorithm already known to the card
P2	'00' = Key reference already known to the card
Lc	'000100' = Length of subsequent data field = 256
Data field	Authentication related data; see Clause 14.7.1 of [HPC-P1]
Le	Absent

Table 38 - (N3040.00) EXTERNAL AUTHENTICATE response

Data field	Absent
SW1-SW2	'9000' or specific status bytes; see [HPC-P1]

In the second part of the procedure the SMC-A proves its authenticity to the counterpart. The software system will require a challenge from the counterpart prior to sending the subsequent command.

Table 39 – (N3041.00) INTERNAL AUTHENTICATE command

CLA	As defined in ISO/IEC 7816-4
INS	'88' = INTERNAL AUTHENTICATE
P1	'00' = Algorithm already known to the card
P2	'00' = Key reference already known to the card
Lc	'000010' = Length of subsequent data field
Data field	Authentication related data; see Clause 14.7.4 of [HPC-P1]
Le	'0100' = Length of expected signature

Table 40 – (N3042.00) INTERNAL AUTHENTICATE response

Data field	Authentication related data; see Clause 14.7.4 of [HPC-P1]
SW1-SW2	'9000' or specific status bytes; see [HPC-P1]

The authentication token (content of the response data field) will be verified in the related counterpart and sets in the counterpart the security status "CHA with profile 54 successfully presented".

The authentication related data contain data elements for key computation. The secure messaging keys are computed as described in Clause 13.1 of [HPC-P1]. The keys are used for production and processing of secure messaging data objects; see Clause 5.9.5 through Clause 5.9.8.

5.9.3 Asymmetric Authentication with Storage of Introduction Keys

In the authentication sequence of agreement on introduction keys, the counterpart receives the first INTERNAL AUTHENTICATE and the SMC-A receives the first EXTERNAL AUTHENTICATE, in order to set in the SMC-A the security status that is required for the use of the private authentication key of the SMC-A. Before the authentication commands are sent to the SMC-A, the key references and the appropriate algorithm identifiers have to be set for external and internal authentication.
Both MSE SET commands for external and internal authentication are performed successively, so that the sequence of authentication commands will not be interrupted by a MSE SET command; see Chapter 15 of [HPC-P1].

Table 41 – (N3043.00) MSE command for key and algorithm selection

CLA	As defined in ISO/IEC 7816-4
INS	'22' = MANAGE SECURITY ENVIRONMENT
P1	'81' = SET for external authentication
P2	'A4' = Authentication Template in data field
Lc	'11' = Length of subsequent data field = 17
Data field	'83 0C xx ... xx' || '80 01 94' = DO KeyRef of PuK.HPC.AUTD_SUK_CVC (HPC) or PuK.SMC.AUTD_RPE_CVC (SMC-B) or PuK.KM.AUTD_RPE_CVC (RFID Token); see Note || DO AlgID rsaSessionkey4Intro
Le	Absent

NOTE – The CHR of the counterpart's CV certificate is used as key reference. It has a length of 12 byte: index set to '00' (1 byte) || KeyRef of private key of counterpart (1 byte) || ICCSN of counterpart (10 byte), see Clause 8.5.2 of [HPC-P1] for CHR structure.

Table 42 – (N3044.00) MSE response

Data field	Absent
SW1-SW2	'9000' or specific status bytes; see [HPC-P1]

Table 43 – (N3045.00) MSE command for key and algorithm selection

CLA	As defined in ISO/IEC 7816-4
INS	'22' = MANAGE SECURITY ENVIRONMENT
P1	'41' = SET for internal authentication
P2	'A4' = Authentication Template in data field
Lc	'06' = Length of subsequent data field = 6
Data field	'84 01 12' || '80 01 94' = DO KeyRef of PrK.SMC.AUTD_RPS_CVC of SMC || DO AlgID rsaSessionkey4Intro
Le	Absent

Table 44 – (N3046.00) MSE response

Data field	Absent
SW1-SW2	'9000' or specific status bytes; see [HPC-P1]

The first part of the procedure comprises the authentication of the counterpart. First, a challenge is retrieved from the SMC-A. Then, an INTERNAL AUTHENTICATE command with RND.SMC || ICCSN8.SMC in the data field has to be sent to the counterpart. The resulting digital signature is presented to the SMC-A in an EXTERNAL AUTHENTICATE command that verifies the counterpart's signature.

Table 45 – (N3047.00) GET CHALLENGE command

CLA	As defined in ISO/IEC 7816-4
INS	'84' = GET CHALLENGE
P1, P2	'0000'
Lc	Absent
Data field	Absent
Le	'08'

Table 46 – (N3048.00) GET CHALLENGE response

Data field	RND.SMC (8 bytes)
SW1-SW2	'9000' or specific status bytes; see [HPC-P1]

Table 47 – (N3049.00) EXTERNAL AUTHENTICATE command

CLA	As defined in ISO/IEC 7816-4
INS	'82' = EXTERNAL AUTHENTICATE
P1	'00' = Algorithm already known to the card
P2	'00' = Key reference already known to the card
Lc	'000100' = Length of subsequent data field = 256
Data field	Authentication related data; see Clause 14.7.1 of [HPC-P1]
Le	Absent

Table 48 – (N3050.00) EXTERNAL AUTHENTICATE response

Data field	Absent
SW1-SW2	'9000' or specific status bytes; see [HPC-P1]

If the authentication was successful, the SMC-A temporarily sets the security status required for the usage of the authentication key PrK.SMC.AUTD_RPS_CVC. The authentication related data contain data elements for key computation. In the second part of the procedure the SMC-A proves its authenticity towards the counterpart. Therefore, the software system has to require a challenge from the counterpart. The challenge is presented to the SMC-A together with the 8 LSB of the counterpart's ICC Serial number in the following INTERNAL AUTHENTICATE command.

Table 49 – (N3051.00) INTERNAL AUTHENTICATE command

CLA	As defined in ISO/IEC 7816-4
INS	'88' = INTERNAL AUTHENTICATE
P1	'00' = Algorithm already known to the card
P2	'00' = Key reference already known to the card
Lc	'000010' = Length of subsequent data field = 16
Data field	Authentication related data; see Clause 14.7.4 of [HPC-P1]
Le	'0100' = Length of expected signature = 256

Table 50 – (N3052.00) INTERNAL AUTHENTICATE response

Data field	Authentication related data; see Clause 14.7.4 of [HPC-P1]
SW1-SW2	'9000' or specific status bytes; see [HPC-P1]

The computed digital signature is presented to the counterpart in an EXTERNAL AUTHENTICATE command.

The introduction keys are derived and their attributes are set during the first command that follows the authentication procedure as described in Clause 13.1 of [HPC-P1]. The CHR of the involved counterpart's CVC certificate is stored as reference of the introduction keys after adjusting the index (first byte of CHR) to the computed key material, i.e. '02' for 3TDES keys; see Clause 8.5.2 of [HPC-P1]. During the derivation of introduction keys the security status is deleted and secure messaging is not enabled. The introduction keys are used in a symmetric authentication, in order to establish session keys for trusted channel, see next clause.

5.9.4 Symmetric Authentication with TC Establishment

If a certain SMC-A and a certain HPC (or SMC-B or RFID Token) have been introduced to each other before, i.e. had performed an asymmetric authentication including the persistent storage of introduction keys, then both cards can perform a symmetric authentication by using the shared introduction keys.

During a successful symmetric authentication the security status “Successful verification of the HPC (SMC-B, RFID Token) role identifier” is set, since the verified role identifier, the used key identifier and the access rule of the private key. have been assigned to the introduction keys during the successful asymmetric authentication; see [HPC-P1], Clause 8.5.2, Clause 13.1.1 and Clause 15.6.

The command sequence at the SMC-A side starts with setting the introduction keys and the appropriate algorithm for mutual authentication.

Table 51 – (N3053.00) MSE command for key and algorithm selection

CLA	As defined in ISO/IEC 7816-4
INS	‘22’ = MANAGE SECURITY ENVIRONMENT
P1	‘81’ = SET for mutual authentication
P2	‘A4’ = Authentication Template in data field
Lc	‘11’ = Length of subsequent data field
Data field	‘83 0C 02 xx ... xx’ || ‘80 01 74’ = DO KeyRef of Introduction keys (3TDES) || DO AlgID desSessionkey4TC
Le	Absent

Table 52 – (N3054.00) MSE response

Data field	Absent
SW1-SW2	‘9000’ or specific status bytes; see [HPC-P1]

NOTE – The key reference has a length of 12 byte: index set to '02' indicating 3TDES introduction keys (1 byte) || KeyRef of PrK.HPC.AUTD_SUK_CVC of HPC or PrK.SMC.AUTD_ RPE_CVC of SMC-B or PrK.KM.AUTD_RPE_CVC of RFID Token (1 byte) || ICCSN of the counterpart (10 byte); see Clause 8.5.2 of [HPC-P1] for structure of the introduction key reference.

After that a challenge is retrieved from the SMC-A.

Table 53 – (N3055.00) GET CHALLENGE command

CLA	As defined in ISO/IEC 7816-4
INS	‘84’ = GET CHALLENGE
P1, P2	‘0000’
Lc	Absent
Data field	Absent
Le	‘08’

Table 54 - (N3056.00) GET CHALLENGE response

Data field	RND.SMC (8 byte)
SW1-SW2	‘9000’ or specific status bytes; see [HPC-P1]

After the GET CHALLENGE command an INTERNAL AUTHENTICATE command with RND.SMC || ICCSN8.SMC in the data field has to be sent to the counterpart. Then, a MUTUAL AUTHENTICATE command follows on the side of the SMC-A. This command delivers the authentication related data of

the counterpart to the SMC-A. The SMC-A has to verify the data of the counterpart and compute the SMC-A authentication related data.

Table 55 – (N3057.00) MUTUAL AUTHENTICATE command

CLA	As defined in ISO/IEC 7816-4
INS	‘82’ = MUTUAL AUTHENTICATE
P1	‘00’ = Algorithm already known to the card
P2	‘00’ = Key reference already known to the card
Lc	‘68’ = Length of subsequent data field = 104
Data field	Authentication related data; see Clause 14.7.1 of [HPC-P1]
Le	‘68’ = Length of expected authentication related data = 104

Table 56 - (N3058.00) MUTUAL AUTHENTICATE response

Data field	Authentication related data; see Clause 14.7.1 of [HPC-P1]
SW1-SW2	‘9000’ or specific status bytes; see [HPC-P1]

The SMC-A authentication related data (content of the response data field) will be verified in the related target card during an EXTERNAL AUTHENTICATE command. A successful verification sets in the target card (HPC, SMC-B or RFID Token) the security status “CHA with profile 54 successfully presented”; see Table (N2624.00) in Annex A.3 of [HPC-P2]. A trusted channel has been established, i.e. data will be transferred to the counterpart in secure messaging mode.

5.9.5 Production of secured Commands using PSO Commands

The support of PSO commands for the production and verification of secure messaging objects is mandatory; see Clause 14.8 of [HPC-P1]. The support of the ENVELOPE command as specified in Clause 5.9.7 is optional. The ENVELOPE command serves as alternative method to support a trusted channel. Whether only the first or both TC support methods are supported, is indicated in the DO Card Capabilities present in EF.ATR; see Table 4 (N3005.00).

The general principles for TC support are described together with the PSO commands in Clauses 13.2, 13.3 and 14.8 of [HPC-P1]. For the SM-DO production the following commands are used:

- PSO: COMPUTE CRYPTOGRAPHIC CHECKSUM
- PSO: ENCIPHER

All commands are sent in normal mode, since the SMC-A does not process secure messaging commands, but produces secure messaging data objects and considers the session keys as "user keys". Since the keys for MAC computation and encipherment and the algorithms to be used are implicitly known, neither key references nor algorithm identifiers have to be set.

Table 57 – (N3059.00) PSO: COMPUTE CRYPTOGRAPHIC CHECKSUM command

CLA	As defined in ISO/IEC 7816-4
INS	‘2A’ = PSO: COMPUTE CRYPTOGRAPHIC CHECKSUM
P1	‘8E’ = CC in response data field
P2	‘80’ = PV in command data field
Lc	‘xx’ or ‘00xxxx’ = Length of subsequent data field
Data field	Data for which the cryptographic checksum shall be computed (command of target card possibly with one of the data objects PV, Le or CG; see also Note)
Le	'00 or ‘0000'

NOTE – The special padding rules as described in Clause “Cryptographic checksum data element” of ISO/IEC 7816-4 have to be applied when constructing the data for the command data field, i.e. the padding bytes have to be inserted; see command description in Clause 14.8.2 of [HPC-P1].

Table 58 – (N3060.00) PSO: COMPUTE CRYPTOGRAPHIC CHECKSUM response

Data field	Cryptographic checksum
SW1-SW2	‘9000’ or specific status bytes; see [HPC-P1]

If in the secured command of the target card enciphered data have to be transmitted (e.g. a PIN), then the computation of the cryptogram is achieved with the PSO: ENCIPHER command, which has to be sent prior to the PSO: COMPUTE CRYPTOGRAPHIC CHECKSUM command.

Table 59 – (N3061.00) PSO: ENCIPHER command

CLA	As defined in ISO/IEC 7816-4
INS	‘2A’ = PSO: ENCIPHER
P1	‘86’ = Padding Indicator || cryptogram in response data field
P2	‘80’ = PV in command data field
Lc	‘xx’ or ‘00xxxx’ = Length of subsequent data field
Data field	Data to encipher
Le	'00' or ‘0000'

Table 60 – (N3062.00) PSO: ENCIPHER response

Data field	'01' (Padding Indicator) || enciphered data
SW1-SW2	‘9000’or specific status bytes; see [HPC-P1]

5.9.6 Processing secured Responses using PSO Commands

For the verification of a cryptographic checksum, the PSO operation VERIFY CRYPTOGRAPHIC CHECKSUM shall be used.

Table 61 – (N3063.00) PSO: VERIFY CRYPTOGRAPHIC CHECKSUM command

CLA	As defined in ISO/IEC 7816-4
INS	‘2A’ = PSO: VERIFY CRYPTOGRAPHIC CHECKSUM
P1	‘00’
P2	‘A2’ = PV in command data field
Lc	‘xx’ or ‘00xxxx'= Length of subsequent data field
Data field	'80'-L-PV || '8E'-L-CC
Le	Absent

Table 62 – (N3064.00) PSO: VERIFY CRYPTOGRAPHIC CHECKSUM response

Data field	Absent
SW1-SW2	‘9000’ or specific status bytes; see [HPC-P1]

If the response data contain a cryptogram, then the deciphered data are obtained with the PSO operation DECIPHER.

Table 63 – (N3065.00) PSO: DECIPHER command

CLA	As defined in ISO/IEC 7816-4
INS	‘2A’ = PSO: DECIPHER
P1	‘80’ = PV in response data field
P2	‘86’ = Padding Indicator || cryptogram in command data field
Lc	‘xx’ or ‘00xxxx' = Length of subsequent data field
Data field	‘01’ (Padding Indicator) || cryptogram
Le	'00' or ‘0000’

Table 64 – (N3066.00) PSO: DECIPHER response

Data field	Deciphered data
SW1-SW2	‘9000’ or specific status bytes; see [HPC-P1]

5.9.7 Production of secured Commands using the ENVELOPE Command (optional)

The strategy in this case is to send as data the command to be secured to the SMC-A and to retrieve the cryptographic checksum DO and possibly also a cryptogram DO, so that the time consumption for producing a secured command is probably reduced. For this purpose, an ENVELOPE command with odd instruction code is send in normal mode to the SMC-A, i.e. the SMC-A considers the ENVELOPE command. The command is described in Clause 14.9.1 of [HPC-P1].

The data field contains the unsecured command in the DO Command-to-perform (tag '52') and an SM template (tag '7D') containing the Response Descriptor (tag 'BA') which denotes, what shall be returned: the SM data object CC and – if needed – also the SM data object CG, encapsulated in an SM Template. The SM template enforces the usage of the SM keys.

NOTE – The ENVELOPE command with odd instruction code allows the construction of such special services.

Table 65 – (N3067.00) ENVELOPE command for the production of the SM-DOs of a secured command

CLA	As defined in ISO/IEC 7816-4
INS	‘C3’ = ENVELOPE
P1-P2	‘0000’
Lc	‘xx’ or ‘00xxxx’ = Length of subsequent data field
Data field	- **Case 1**: If the command to be secured contains data to be transmitted in DO PV: '52'-L-command to be secured || '7D'-L-('BA'-L-['8E'-'00']) - **Case 2**: If the command to be secured contains data to be transmitted in a DO CG: '52'-L-command to be secured || '7D'-L-('BA'-L-['87'-'00' || '8E'-'00'])
Le	'00' or ‘0000’

Table 66 – (N3068.00) ENVELOPE response

Data field	- Case 1: '7D'-L-('8E'-'08'-CC) - Case 2: '7D'-L-('87'-L-'01'-CG || '8E'-'08'-CC)
SW1-SW2	‘9000’ or specific status bytes; see [HPC-P1]

For the CC computation, the value field of the DO ‘Command-to-perform’ (tag ‘52’) shall be taken applying the rules for CC computation for SM-protected commands as defined in [ISO7816-4], whereby the command header shall be always integrated in the CC.

5.9.8 Processing of secured Responses using the ENVELOPE Command (optional)

For the processing of a secured response APDU, 3 cases have to be distinguished:

- Response with DO Status bytes (tag '99')
- Response with DO Plain value (tag '81') and DO Status bytes (tag '99')
- Response with DO Cryptogram (tag '87') and DO Status bytes (tag '99').

NOTE – The cases addressed here are application cases and should not be mixed up with transmission cases of command-response pairs as described in ISO/IEC 7816-3.

All secured responses are protected by a cryptographic checksum CC. The CC has to be verified. If a cryptogram is present, then the plain value has to be returned by the SMC-A after successful verification of the CC. The command is described in Clause 14.9.1 of [HPC-P1].

Table 67 – (N3069.00) ENVELOPE command for the processing of the SM-DOs of a secured response

CLA	As defined in ISO/IEC 7816-4
INS	‘C3’ = ENVELOPE
P1-P2	‘0000’
Lc	‘xx’ or ‘00xxxx’ = Length of subsequent data field
Data field	- **Case 1**: Response APDU with DO Processing status and DO CC '7D'-L-('99'-'02'-SW1-SW2 || '8E'-'08'-CC) - **Case 2**: Response APDU with DO Plain value, DO Processing status and DO CC: '7D'-L-('81'-L-Data || '99'-'02'-SW1-SW2 || '8E'-'08'-CC) - **Case 3**: Response APDU with DO Cryptogram, DO Processing status and DO CC: '7D'-L-('87'-L-'01'-CG || '99'-'02'-SW1-SW2 || '8E'-'08'-CC || ‘BA'-L-['80'-'00'])
Le	Case 1, 2: Absent Case 3: '00' or ‘0000’

Table 68 – (N3070.00) ENVELOPE response

Data field	- Case 1, 2: Absent - Case 3: '7D'-L-('80'-L-Data, which have been deciphered)
SW1-SW2	‘9000’or specific status bytes; see [HPC-P1]

5.10 The Security Module Application

5.10.1 File Structure and File Content

The file structure of DF.SMA for SMC-A is shown in the subsequent Figure.

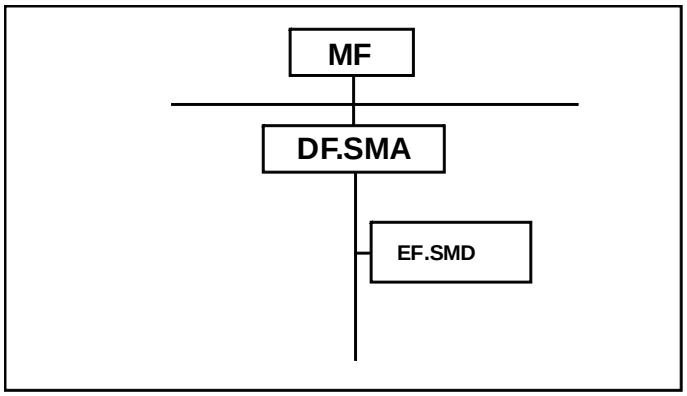

Figure 3 - (N3071.00) File structure of DF.SMA in SMC-A

For SMC-A, neither EF.CONF nor EF.NET is present under DF.SMA.

5.10.1.1 DF.SMA (Security Module Application)

DF.SMA is an application according to Clause 8.3.1.1 of [HPC-P1], i.e. selectable by using the application identifier. Table 69 (N3072.00) shows the characteristics of the application directory.

Table 69 – (N3072.00) Characteristics of MF / DF.SMA

Attribute	**Value**	**Note**
Object type	Application Directory	
Application Identifier	‘D27600014605’	
File Identifier	-	Manufacturer-specific; if supported, then out of interval [‘1000’, ‘FEFF’]; see Clause 8.1.1 of [HPC-P1]
Life Cycle Status	Operational state (activated)	
Access Rule in all SEs		
Access Mode	**Security Condition**	**Note**
SELECT	ALWAYS	
LOAD APPLICATION (after SMC-A issuing)	AUT(‘D27600014600' || '01') AND SmMac AND SmCmdEnc	Only executable if a CAMS is used; see Clause 5.12. If a CAMS with symmetric authentication is used, then the security condition must contain the key reference of the corresponding symmetric key, i.e. AUT('13') instead of AUT(‘D27600014600' || '01’).
ACTIVATE, DEACTIVATE, DELETE	NEVER	

The keys and CVCs for the authentication procedure are placed at the MF level. The SMA allows the installation of further files due to possibly upcoming needs; see Clause 5.12.

5.10.1.2 EF.SMD

The transparent file EF.SMD is intended to be used for storing SMC-A related data, e.g. special configuration data. The file can be read always. An update is only possible after successful execution of an authentication procedure between the SMC-A and a related HPC or SMC. The attributes and access conditions of EF.SMD are shown in the subsequent table.

Table 70 – (N3073.00) Characteristics of MF / DF.SMA / EF.SMD

Attribute	**Value**	**Note**
Object type	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	...	
Access Rule in all SEs		
Access Mode	**Security Condition**	**Note**
SELECT, READ BINARY	ALWAYS	
UPDATE BINARY, ERASE BINARY	AUT('D27600004000' || 'xx')	Role authentication of HPC or SMC with related personal profile, e.g. profile 2; see [HPC-P2], Table (N2623.00).
ACTIVATE, DEACTIVATE, DELETE	NEVER	

5.10.2 Security Environments at DF Level

In DF.SMA only SE # 1 (default SE) is used. It is possible in SE # 1 to establish a trusted channel, e.g. for online data processing in future applications.

5.10.3 Application Selection

The application selection is performed with the ISO/IEC 7816-4 SELECT command as shown in the subsequent two tables.

Table 71 - (N3074.00) SELECT command for DF.SMA

CLA	As defined in ISO/IEC 7816-4
INS	'A4' = SELECT
P1	'04' = DF selection by AID
P2	'0C' = No FCI to return
Lc	'06' = Length of subsequent data field
Data field	'D27600014605' = AID of DF.SMA of SMC-A
Le	Absent

Table 72 - (N3075.00) SELECT response

Data field	Absent
SW1-SW2	'9000' or specific status bytes; see [HPC-P1]

5.10.4 Reading, Updating and Erasing Data of EF.SMD

For reading EF.SMD the ISO/IEC 7816-4 command READ BINARY is used.

Table 73 - (N3076.00) READ BINARY command for reading EF.SMD with SFID

CLA	As defined in ISO/IEC 7816-4
INS	'B0' = READ BINARY
P1, P2	- P1 = b8-b6: 100 b5-b1: 0001 SFID of EF.SMD: 1 P2 = Offset - 'xxxx' = Offset (bit b8 of P1 = 0)
Lc	Absent
Data field	Absent
Le	'00' or '000000' = Read until end-of-file

Table 74 - (N3077.00) READ BINARY response

Data field	Data
SW1-SW2	'9000' or specific status bytes; see [HPC-P1]

If the supported extended length is not sufficient to read the data with a single command, the READ BINARY command shall be repeated specifying the respective offset in P1-P2.

For updating EF.SMD the ISO/IEC 7816-4 command UPDATE BINARY is used. The required security status for the update operation is the successful HPC or SMC authentication; see Table 70 (N3073.00).

Table 75 - (N3078.00) UPDATE BINARY command for updating EF.SMD

CLA	As defined in ISO/IEC 7816-4
INS	'D6' = UPDATE BINARY
P1, P2	- P1 = b8-b6:100 b5-b1: 00001 SFID of EF.SMD: 1 P2 = Offset - 'xxxx' = Offset (bit b8 of P1 = 0)
Lc	'xx' or '00xxxx' = Length of subsequent data field
Data field	Data
Le	Absent

Table 76 - (N3079.00) UPDATE BINARY response

Data field	Absent
SW1-SW2	'9000' or specific status bytes; see [HPC-P1]

If the supported extended length is not sufficient to write the data with a single command, the UPDATE BINARY command shall be repeated specifying the respective offset in P1-P2.

For erasing the data in EF.SMD the ISO/IEC 7816-4 command ERASE BINARY is used; see Table 77 (N3080.00). The command deletes data by replacing the data bytes with '00' bytes; see Clause 14.3.1 of [HPC-P1]. The required security status for the erase operation is the successful HPC or SMC authentication; see Table 70 (N3073.00).

Table 77- (N3080.00) ERASE BINARY command for deleting data in EF.SMD

CLA	As defined in ISO/IEC 7816-4
INS	'0E' = ERASE BINARY
P1, P2	- P1 = b8-b6:100 b5-b1: 00001 SFID of EF.SMD: 1 P2 = Offset - 'xxxx' = Offset (bit b8 of P1 = 0)
Lc	Absent
Data field	Absent
Le	Absent

Table 78 - (N3081.00) ERASE BINARY response

Data field	Absent
SW1-SW2	'9000' or specific status bytes; see [HPC-P1]

If the supported extended length is not sufficient to erase the data with a single command, the ERASE BINARY command shall be repeated specifying the respective offset in P1-P2.

5.11 The KT-Application (Card Terminal Application)

5.11.1 File Structure and File Content

DF.KT is used for:

- authentication for connecting the card terminal to a specific connector.

The file-structure of DF.KT for SMC-A is shown in the subsequent figure.

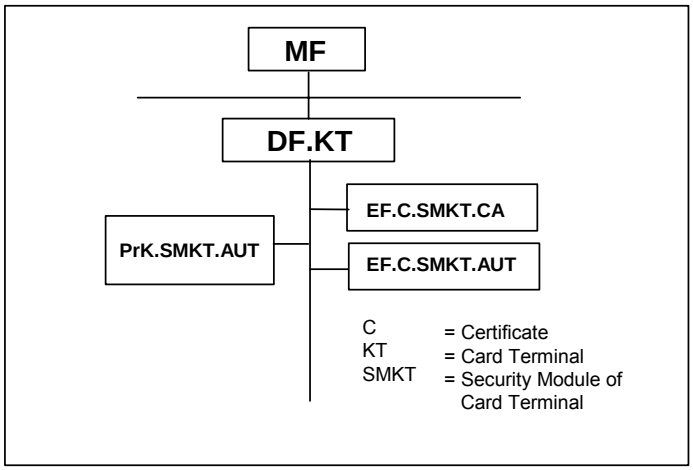

Figure 4 – (N3082.00) File Structure of DF.KT

It shall be possible to use the functionality of DF.KT in more than one logical channel, i.e. the functionality provided by DF.KT shall be shareable.

5.11.1.1 DF.KT (Card Terminal Application)

DF.KT is an application according to Clause 8.3.1.1 of [HPC-P1], i.e. selectable by using the application identifier. Table 79 (N3083.00) shows the characteristics of the application directory.

Table 79 – (N3083.00) Characteristics of MF / DF.KT

Attribute	**Value**	**Note**
Object type	Application Directory	
Application Identifier	'D27600014400'	Application of gematik
File Identifier	-	Manufacturer-specific; if supported, then out of interval ['1000', 'FEFF']; see Clause 8.1.1 of [HPC-P1]
Life Cycle Status	Operational state (activated)	
Access Rule in all SEs		
Access Mode	**Security Condition**	**Note**
SELECT	ALWAYS	
LOAD APPLICATION, ACTIVATE, DEACTIVATE, DELETE	NEVER	

5.11.1.2 EF.C.SMKT.CA

EF.C.SMKT.CA contains the X.509 certificate of the Certification Authority (CA) which is the issuer of the X.509-certificate C.SMKT.AUT. File ID and access conditions are specified in Table 80 (N3084.00).

Table 80 – (N3084.00) Characteristics of MF / DF.KT / EF.C.SMKT.CA

Attribute	**Value**	**Note**
Object type	Transparent Elementary File	
File Identifier	'C502'	
Short File Identifier	'02' = 2	
Number of Bytes	1536 or limited to length of certificate	
Flag Transaction Mode	False	
Flag Checksum	False	
Life Cycle Status	Operational state (activated)	
Content	...	To be personalized.
Access Rule in all SEs		
Access Mode	**Security Condition**	**Note**
SELECT, READ BINARY	ALWAYS	
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, UPDATE BINARY	NEVER	

5.11.1.3 EF.C.SMKT.AUT

EF.C.SMKT.AUT contains the X.509 certificate for authentication. File IDs and access conditions are specified in Table 81 (N3085.00).

Table 81 – (N3085.00) Characteristics of MF / DF.KT / EF.C.SMKT.AUT

Attribute	Value	Note
Object type	Transparent Elementary File	
File Identifier	'C501'	
Short File Identifier	'01' = 1	
Number of Bytes	1536 or limited to length of certificate	
Flag Transaction Mode	False	
Flag Checksum	False	
Life Cycle Status	Operational state (activated)	
Content	...	To be personalized
Access Rule in all SEs		
Access Mode	**Security Condition**	**Note**
SELECT, READ BINARY	ALWAYS	
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, UPDATE BINARY	NEVER	

5.11.1.4 PrK.SMKT.AUT

PrK.SMKT.AUT is the private authentication key for connecting the card terminal to a specific connector. The key characteristics are shown in the subsequent table.

Table 82 – (N3086.00) Characteristics of MF / DF.KT / PrK.SMKT.AUT

Attribute	Value	Note
Object type	Private RSA Object	
Key Identifier	'02' = 2	
Key Reference	'82'	
Private Key	.... (2048 bit)	To be personalized
Key Available	True	
Algorithm Identifier	rsaDecipherPKCS1_V1_5 signPKCS1_V1_5	
Access Rule in all SEs		
Access Mode	**Security Condition**	**Note**
PSO: DECIPHER	ALWAYS	
INTERNAL AUTHENTICATE	ALWAYS	
Other	NEVER	

5.11.2 Security Environments at DF Level

In DF.KT only SE # 1 (default SE) is used. It is possible in SE # 1 to establish a trusted channel, e.g. for online data processing in future applications.

5.11.3 Application Selection

The application selection is performed with the ISO/IEC 7816-4 SELECT command as shown in the subsequent two tables.

Table 83 - (N3087.00) SELECT command

CLA	As defined in ISO/IEC 7816-4
INS	‘A4’ = SELECT
P1	‘04’ = DF selection by AID
P2	‘0C’ = No FCI to return
Lc	‘06’ = Length of subsequent data field
Data field	´D27600014400´ = AID of DF.KT
Le	Absent

Table 84 - (N3088.00) SELECT response

Data field	Absent
SW1-SW2	‘9000’ or specific status bytes; see [HPC-P1]

5.11.4 Reading X.509 Certificates

The reading of X.509 certificates is described in Clause 10.4 of [HPC-P2].

5.11.5 Generating a Random Number

For generating a cryptographically secure random number the command GET RANDOM is used as specified in Clause 14.9.7 of [HPC-P1].

Table 85 - (N3089.00) GET RANDOM command

CLA	As defined in ISO/IEC 7816-4 for proprietary class
INS	‘84’ = GET RANDOM (identical to GET CHALLENGE)
P1, P2	‘0000’
Lc	Absent
Data field	Absent
Le	‘xx’ = length of expected random number in the response data

Table 86 - (N3090.00) GET RANDOM response

Data field	Random number
SW1-SW2	‘9000’ or specific status bytes; see [HPC-P1]

The generated random number is not available for further operations inside the card.

5.11.6 Using the Private Key

The private key PrK.SMKT.AUT can be used without PIN entry. For deciphering an enciphered secret the private key and the algorithm have to be selected with the ISO/IEC 7816-4 command MSE.

Table 87 - (N3091.00) MSE command for key and algorithm selection

CLA	As defined in ISO/IEC 7816-4
INS	‘22’ = MANAGE SECURITY ENVIRONMENT
P1	‘41’ = SET for decipherment
P2	‘B8’ = Confidentiality Template
Lc	‘06’ = Length of subsequent data field
Data field	’84 01 82’ || ’80 01 81’ = DO KeyRef of PrK.SMKT.AUT || DO AlgID rsaDecipherPKCS1_V1_5
Le	Absent

Table 88 - (N3092.00) MSE response

Data field	Absent
SW1-SW2	‘9000’ or specific status bytes; see [HPC-P1]

After the key and the algorithm have been set, the decipher operation can be executed with the ISO/IEC 7816-8 command PSO: DECIPHER.

Table 89 – (N3093.00) PSO: DECIPHER command

CLA	As defined in ISO/IEC 7816-4
INS	‘2A’ = PERFORM SECURITY OPERATION: DECIPHER
P1	‘80’ = Return plain value
P2	‘86’ = Enciphered data present in the data field
Lc	‘000101’ = Length of subsequent data field = 257
Data field	‘00’ (Padding indicator) || cryptogram (256 bytes)
Le	‘0000’ or ‘00xx’ = Length of the deciphered secret

Table 90 – (N3094.00) PSO: DECIPHER response

Data field	Deciphered secret
SW1-SW2	‘9000’or specific status bytes; see [HPC-P1]

For computing authentication related data the INTERNAL AUTHENTICATE command is used. Before this command can be executed, the private key and the appropriate algorithm identifier have to be set.

Table 91 – (N3095.00) MSE command for key and algorithm selection

CLA	As defined in ISO/IEC 7816-4
INS	‘22’ = MANAGE SECURITY ENVIRONMENT
P1	‘41’ = SET for internal authentication
P2	‘A4’ = Authentication Template
Lc	‘06’ = Length of subsequent data field
Data field	‘84 01 82’ || ’80 01 02’ = DO KeyRef of PrK.SMKT.AUT || DO AlgID signPKCS1_V1_5
Le	Absent

Table 92 - (N3096.00) MSE response

Data field	Absent
SW1-SW2	'9000' or specific status bytes; see [HPC-P1]

Table 93 - (N3097.00) INTERNAL AUTHENTICATE command

CLA	As defined in ISO/IEC 7816-4
INS	'88' = INTERNAL AUTHENTICATE
P1	'00'
P2	'00'
Lc	'00xxxx' = Length of subsequent data field
Data field	Authentication related data; see Clause 14.7.4 of [HPC-P1]
Le	'0100' = length of expected digital signature = 256

Table 94 - (N3098.00) INTERNAL AUTHENTICATE response

Data field	Digital signature
SW1-SW2	'9000' or specific status bytes; see [HPC-P1]

5.12 Loading a new Application or Creation of an EF after SMC-A Issuing

It is assumed that the loading of a new application or creation of new EFs on MF level (including updating the files EF.DIR and EF.Version) or the creation of a new EF in DF.SMA after issuing of the SMC-A is performed by a Card Application Management System (CAMS). This is an optional procedure.

Similarly, a CAMS is optional. The content of Chapter 13 of [HPC-P2] is however normative, if loading of a new application or creation of a new EF after SMC-A issuing are to be performed.

6 Security Module Card B

6.1 ATR coding and Technical Characteristics

For the SMC-B the same conventions apply for the technical characteristics, Answer-to-Reset and transmission protocols as for the HPC and SMC-A. See Chapter 11.2 of [HPC-P1] for the electrical interface and Clause 4.1 of [HPC-P2] for ATR coding. The SMC-B is designed for use as plug-in card (ID-000) present in related card terminals.

6.2 General Structure

The SMC-B contains

- the Root Application (MF) with some EFs at MF level for general data objects, CV certificates, global keys and PIN for authentication procedures (e.g. proving access rights to the eGK and verification of the authenticity of the eGK),
- the Security Module Application (DF.SMA) for the provision of SMC-B related data file(s) and files for configuration data of the connector and the network,
- the ESIGN Application (DF.ESIGN) with PKI keys for organizational signatures, client/server authentication, decipherment and transcipherment of documents,
- the Card Terminal Application (DF.KT) for authentication of the card terminal to connect to a specific connector.

The general structure of SMC-B is shown in Figure 5 (N3500.00)

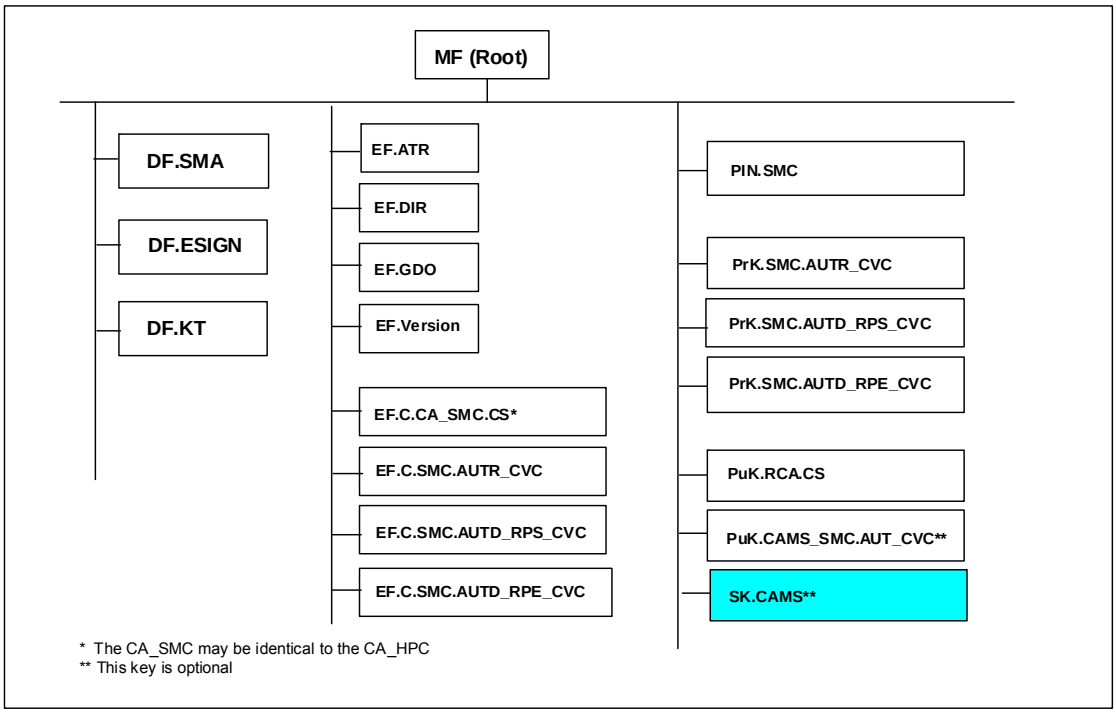

Figure 5 – (N3500.00) General structure of the SMC-B

The functionality of SMC-B covers the full functionality of SMC-A. All EFs of SMC-A are also present in SMC-B. Additionally on MF level of SMC-B, a further CVC for device authentication, the corresponding private key and an SMC-B related PIN are available.

Furthermore, the ESIGN application for PKI services is available in the SMC-B. A cryptographic information application (DF.CIA.ESIGN) is not necessary, since an SMC-B remains stationary and the respective software knows the usage conventions.

6.3 Root Application and Elementary Files at MF Level

6.3.1 MF

The MF of SMC-B is an Application Dedicated File (see Clause 8.3.1.3 of [HPC-P1]) and has got the characteristics shown in Table 95 (N3501.00).

Table 95 – (N3501.00) Characteristics of MF

Attribute	Value	Note
Object type	Application Dedicated File	
Application Identifier	‘D27600014606’	
File Identifier	‘3F00’	Optional
Life Cycle Status	Operational state (activated)	
Access Rule in all SEs		
Access Mode	**Security Condition**	**Note**
SELECT	ALWAYS	
LOAD APPLICATION (after SMC-B issuing)	AUT('D27600014600' || '01') AND SmMac AND SmCmdEnc	Only executable if a CAMS is used; see Clause 5.12. If a CAMS with symmetric authentication is used, then the security condition must contain the key reference of the corresponding symmetric key, i.e. AUT('13') instead of AUT(‘D27600014600' || '01’).
ACTIVATE, DEACTIVATE, DELETE	NEVER	

6.3.2 EF.ATR

Characteristics and usage of EF.ATR are the same as for SMC-A; see Clause 5.3.2.

6.3.3 EF.DIR

EF.DIR contains the application templates for MF, DF.SMA, DF.ESIGN, and DF.KT according to ISO/IEC 7816-4. EF.DIR allows the addition of AIDs of further (downloaded) applications; see the following table for characteristics of EF.DIR.

Table 96 – (N3502.00) Characteristics of MF / EF.DIR

Attribute	Value	Note
Object type	Linear Variable Record Elementary File	
File Identifier	‘2F00’	
Short File Identifier	‘1E’ = 30	
Number of Bytes	133	7 * max. record length
Maximum Number of Records	7 (3 for future use)	
Maximum Record Length	19 bytes	
Flag Record LCS	False	
Flag Transaction Mode	True	
Flag Checksum	True	
Life Cycle Status	Operational state (activated)	
Content	...	see Table 97 (N3503.00)

Access Rule in all SEs		
Access Mode	**Security Condition**	**Note**
SELECT, READ RECORD, SEARCH RECORD	ALWAYS	
APPEND RECORD, UPDATE RECORD	AUT('D27600014600' || '01') AND SmMac	Only executable if a CAMS is used; see Clause 5.12. If a CAMS with symmetric authentication is used, then the security condition must contain the key reference of the corresponding symmetric key, i.e. AUT('13') instead of AUT('D27600014600' || '01').
ACTIVATE, ACTIVATE RECORD, DEACTIVATE, DEACTIVATE RECORD, DELETE, ERASE RECORD	NEVER	

The application templates contained in EF.DIR are shown in Table 97 (N3503.00).

Table 97 – (N3503.00) Application Templates in EF.DIR of SMC-B

Tag	L	Application Template	Meaning
'61'	'08'	'4F 06 D27600014606'	Application Template with AID.MF
'61'	'08'	'4F 06 D27600014607'	Application Template with AID.SMA
'61'	'0C'	'4F 0A A000000167 455349474E'	Application Template with AID.ESIGN
'61'	'08'	'4F 06 D27600014400'	Application Template with AID.KT

6.3.4 EF.GDO

Characteristics and usage of EF.GDO are the same as for SMC-A; see Clause 5.3.4.

6.3.5 EF.Version

Characteristics and usage of EF.Version are the same as for SMC-A; see Clause 5.3.5.

6.3.6 EF.C.CA_SMC.CS

Characteristics and usage of EF.C.CA_SMC.CS and contained CV certificate are the same as for SMC-A; see Clause 5.3.6.

6.3.7 EF.C.SMC.AUTR_CVC

Characteristics and usage of EF.C.SMC.AUTR_CVC and contained CV certificate are the same as for SMC-A; see Clause 5.3.7.

6.3.8 EF.C.SMC.AUTD_RPS_CVC

Characteristics and usage of EF.C.SMC.AUTD_RPS_CVC and contained CV certificate are the same as for SMC-A; see Clause 5.3.8.

6.3.9 EF.C.SMC.AUTD_RPE_CVC

EF.C.SMC.AUTD_RPE_CVC contains the card verifiable certificate for card-to-card device authentication between SMC-B/SMC-A as well as SMC-B/SMC-B with one SMC-B as remote PIN receiver. The characteristics of the file are shown in the following table.

Table 98 – (N3504.00) Characteristics of MF / EF.C.SMC.AUTD_RPE_CVC

Attribute	Value	Note
Object type	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	...	see Table (N2021.00) of [HPC-P2]
Access Rule in all SEs		
Access Mode	**Security Condition**	**Note**
SELECT, READ BINARY	ALWAYS	
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, UPDATE BINARY	NEVER	

The structure and content of the CVC in EF.C.SMC.AUTD_RPE_CVC with CPI = '22' are defined in Clause 7.1.3 of [HPC-P1] and outlined in Table (N2021.00) of [HPC-P2]. The Certificate Holder Authorization relevant for a C.SMC.AUTD_RPE_CVC is shown in Table (N2624.00) of Annex A.3 of [HPC-P2].

6.3.10 PIN.SMC

PIN.SMC is the global PIN of the SMC-B that is used for:

- the authorization of the SMC-B which is linked to the access rule of the private authentication key PrK.SMC.AUTR_CVC; see Table 100 (N3506.00),
- the updating of security module application data in EF.SMD; see Table 107 (N3514.00), and
- the PKI services of the ESIGN application.

The usage of the 8 digit resetting code (personal unblocking key, PUK) is limited by a usage counter with an initial value of 10. The usage counter is decremented irrespective of whether the resetting code was correct or not. The PIN characteristics are shown in the subsequent table.

Table 99 – (N3505.00) Characteristics of MF / PIN.SMC

Attribute	Value	Note
Object type	Password	
Password Identifier	'01'	
Password Reference	'01'	
Secret	....	To be personalized
Minimum Length	6	
Start Retry Counter	3	
Retry Counter	3	
Transport Status	Transport PIN Random or Transport PIN Derived or Transport PIN Fixed Value or Regular Password	To be personalized
Flag Enabled	True	
Start Security Status Evaluation Counter	Infinite	
PUK	...	To be personalized
PUK Usage	10	
Access Rule in all SEs		

Access Mode	Security Condition	Note
CHANGE RD (Option ‘00’)	ALWAYS	
GET PIN STATUS	ALWAYS	
RESET RC (Option ‘00’ and ‘01’)	ALWAYS	
VERIFY	ALWAYS	
Other	NEVER	

The PIN management functions are the same as for PIN.CH of the HPC; see Clause 4.3.9 and Clause 4.6 of [HPC-P2].

6.3.11 PrK.SMC.AUTR_CVC

PrK.SMC.AUTR_CVC is the global private key for C2C-authentication between SMC/eGK. The characteristics of the private authentication key are shown in the subsequent table.

Table 100 – (N3506.00) Characteristics of MF / PrK.SMC.AUTR_CVC

Attribute	Value	Note
Object type	Private RSA Object	Profile 0 or 2 or 3 or ...
Key Identifier	‘10’	
Key Reference	‘10’	
Private Key	.... (2048 bit)	To be personalized
Algorithm Identifier	rsaRoleAuthentication, rsaSessionkey4SM rsaSessionkey4TC	
Access Rule in all SEs		
Access Mode	**Security Condition**	**Note**
INTERNAL AUTHENTICATE	PWD(PIN.SMC) OR AUT(‘D27600004000’ || 'xx')	PIN.SMC or role authentication of HPC with related personal profile, e.g. profile 2; see [HPC-P2], Table (N2623.00)
EXTERNAL AUTHENTICATE	ALWAYS	
Other	NEVER	

The public key associated with PrK.SMC.AUTR_CVC (with CVC holder profile 2 or 3 or...) is contained in C.SMC.AUTR_CVC.

6.3.12 PrK.SMC.AUTD_RPS_CVC

PrK.SMC.AUTD_RPS_CVC is the global private key for C2C-authentication between SMC/HPC, SMC/SMC, or SMC/RFID Token in the context of sending a PIN. The characteristics of the private authentication key are shown in the subsequent table.

Table 101 – (N3507.00) Characteristics of MF / PrK.SMC.AUTD_RPS_CVC

Attribute	Value	Note
Object type	Private RSA Object	Profile 54 (PIN Sender)
Key Identifier	‘12’	
Key Reference	‘12’	
Private Key	.... (2048 bit)	To be personalized
Algorithm Identifier	rsaSessionkey4TC rsaSessionkey4Intro	
Access Rule in all SEs		
Access Mode	**Security Condition**	**Note**
INTERNAL AUTHENTICATE	AUT(‘D27600004000’ || '35') OR AUT(‘D27600004000’ || '37')	Device authentication of HPC (SSCD with profile 53) or SMC or RFID Token (Remote PIN receiver

		with profile 55); see [HPC-P2], Table (N2624.00).
EXTERNAL AUTHENTICATE	ALWAYS	
Other	NEVER	

The public key associated with PrK.SMC.AUTD_RPS_CVC (with CVC holder profile 54) is contained in C.SMC.AUTD_RPS_CVC.

6.3.13 PrK.SMC.AUTD_RPE_CVC

PrK.SMC.AUTD_RPE_CVC is the global private key for C2C-authentication between SMC/SMC in the context of receiving a PIN. The characteristics of the private authentication key are shown in the subsequent table.

Table 102 – (N3508.00) Characteristics of MF / PrK.SMC.AUTD_RPE_CVC

Attribute	**Value**	**Note**
Object type	Private RSA Object	Profile 55 (PIN Receiver)
Key Identifier	'11'	
Key Reference	'11'	
Private Key	.... (2048 bit)	To be personalized
Algorithm Identifier	rsaRoleAuthentication rsaSessionkey4SM rsaSessionkey4Intro	
Access Rule in all SEs		
Access Mode	**Security Condition**	**Note**
INTERNAL AUTHENTICATE	ALWAYS	
EXTERNAL AUTHENTICATE	ALWAYS	
Other	NEVER	

The public key associated with PrK.SMC.AUTD_RPE_CVC (with CVC holder profile 55) is contained in C.SMC.AUTD_ RPE_CVC.

6.3.14 PuK.RCA.CS

PuK.RCA.CS is the public key of the Root CA. Characteristics and usage of the key are the same as for SMC-A; see Table 20 (N3022.00) in Clause 5.3.11.

6.3.15 PuK.CAMS_SMC.AUT_CVC

PuK.CAMS_SMC.AUT_CVC (optional) is the public key of the SMC-B related Card Application Management System. Characteristics and usage of the key are the same as for SMC-A; see Table 21 (N3023.00) in Clause 5.3.12.

6.3.16 SK.CAMS

SK.CAMS (optional) is the secret key for performing an SMC-B / CAMS authentication procedure with TC establishment. The subsequent table shows the characteristics of the key.

Table 103 – (N3509.00) Characteristics of MF / SK.CAMS

Attribute	**Value**	**Note**
Object type	3TDES Authentication Object	
Key Identifier	'13' = 19	
encKey	...	To be personalized
macKey	...	To be personalized

Algorithm Identifier	desSessionkey4SM	
Access Rule in all SEs		
Access Mode	**Security Condition**	**Note**
MUTUAL AUTHENTICATE	PWD(PIN.SMC) OR AUT('D27600004000' || 'xx')	Authentication with PIN.SMC or role authentication of HPC or SMC with related personal profile, e.g. profile 2; see [HPC-P2], Table (N2623.00).
Other	NEVER	

6.4 Security Environments at MF Level

At MF level only SE # 1 (default SE) is used. It is possible in SE # 1 to establish a trusted channel, e.g. for PIN transfer to the RFID Token or for online data processing in future applications.

6.5 SMC-B Opening

6.5.1 Selecting the Root Application

After reset the root application is selected by default. Afterwards, the root application can be selected, e.g. by using the SELECT command with application identifier as shown in Table 104 (N3510.00).

Table 104 - (N3510.00) SELECT command for MF selection

CLA	As defined in ISO/IEC 7816-4
INS	'A4' = SELECT
P1	'04' = DF selection by AID
P2	'0C' = No FCI to return
Lc	'06' = Length of AID in the data field
Data field	'D27600014606' = AID of Root Application (MF) of SMC-B
Le	Absent

Table 105 - (N3511.00) SELECT response

Data field	Absent
SW1-SW2	'9000' or specific status bytes; see [HPC-P1]

NOTE – The optional FID '3F00' is not used for MF selection since only the current directory is searched for the file identifier; see Clause 14.2.6.10 of [HPC-P1].

6.5.2 Reading EF.ATR and EF.GDO

For reading EF.ATR and EF.GDO, the READ BINARY command is used; see Clause 4.5.3 of [HPC-P2]. Since the SMC-B remains in the respective device, this command is possibly performed only once.

6.5.3 Reading EF.DIR and EF.Version

For reading EF.DIR and EF.Version, the READ RECORD command is used; see Clause 4.5.4 of [HPC-P2]. Since the SMC-B remains in the respective device, this command is possibly performed only once.

6.5.4 Reading SMC-B related CV Certificates

For reading SMC-B related CV Certificates, the READ BINARY command is used; see Clause 4.5.5 of [HPC-P2]. Since the SMC-B remains in the respective device, this command is possibly performed only once by the software environment, which stores the CVCs e.g. associated with the respective CHR of the SMC-B.

6.6 Channel Management

As is the case for the SMC-A, the SMC-B shall support at least 4 logical channels; see Clause 11.4 of [HPC-P1]. The maximum number of logical channels is indicated in EF.ATR; see 5.3.2. Each channel has its own independent security status, i.e. the external authentication of a role identifier in one channel does not set a security status in any other channel.

The channel management shall be performed as specified in Chapter 5 of [HPC-P2].

6.7 Authorization of the SMC-B

The general aspects of the authorization process from the perspective of the authorizing card are outlined in Clause 7.6 of [HPC-P2]. As for the SMC-A, the authorization of the SMC-B is technically mapped to the access rule of PrK.SMC.AUTR_CVC (see Table 100 (N3506.00)) that is used in card-to-card authentication procedures.

The authorization can be achieved by an external authentication of an HPC with the appropriate role ID present in the CHA of the respective card verifiable certificate for role authentication (C.HPC.AUTR_CVC); see Table (N2623.00) in Annex A.3 of [HPC-P2]. The authorization procedure described in Clause 5.7 for the SMC-A can be applied also to the SMC-B.

Alternatively, the SMC-B can be authorized by successful presentation of PIN.SMC; see Clause 6.3.10.

6.8 Interactions between SMC-B and eGK

If there is no SMC-A available, e.g. in a small institution, the SMC/eGK authentication with or without TC establishment may be performed with an SMC-B instead of an SMC-A. The keys and algorithms used in these interactions are the same as described in Clause 5.8 for the SMC-A.

6.9 Interactions between SMC-B and SMC-A or RFID Token

6.9.1 General

An overview of the possible authentication procedures between SMC/HPC, SMC/SMC and SMC/ RFID Token is given in Clause 7.1 of [HPC-P2]. Like the SMC-A the SMC-B supports the GET SECURITY STATUS KEY command for querying e.g. the authentication status of a specified role identifier; see Clause 7.2 of [HPC-P2].

The SMC-B in the role of PIN sender uses the corresponding private authentication key for device authentication, PrK.SMC.AUTD_RPS_CVC (profile 54), to interact with an RFID Token.

The SMC-B in the role of PIN receiver uses the corresponding private authentication key for device authentication, PrK.SMC.AUTD_RPE_CVC (profile 55), to interact with an SMC-A which on its part acts as PIN sender.

Before an asymmetric procedure can be performed, the CVCs of the SMC-B must have been read; see Clause 5.5.4. The CV certificates related to the counterpart are to be verified, so that the corresponding public keys will be available in the SMC-B.

6.9.2 Asymmetric Authentication with TC establishment as PIN Sender

The private key PrK.SMC.AUTD_RPS_CVC has to be activated by external authentication of the related PIN receiving card, i.e. an RFID Token. This is part of the authentication procedure that is performed as described in Clause 5.9.2. For this purpose, RSA authentication with agreement on session keys for trusted channel is set as algorithm in the SMC-B.

6.9.3 Asymmetric Authentication with storage of introduction keys as PIN Sender

The private key PrK.SMC.AUTD_RPS_CVC has to be activated by external authentication of the related PIN receiving card, i.e. an RFID Token. This is part of the authentication procedure as described in Clause 5.9.3. For this purpose, RSA authentication with agreement on introduction keys is set as algorithm in the SMC-B.

6.9.4 Asymmetric Authentication with TC establishment as PIN Receiver

The authentication procedure uses the private key PrK.SMC.AUTD_RPE_CVC as described in Clause 7.3 of [HPC-P2] with the SMC-B taking the place of the HPC towards a related PIN sending card, i.e. an SMC-A. For this purpose, RSA authentication with agreement on session keys for secure messaging is set as algorithm in the SMC-B.

6.9.5 Asymmetric Authentication with storage of introduction keys as PIN Receiver

The authentication procedure uses the private key PrK.SMC.AUTD_RPE_CVC as described in Clause 7.4 of [HPC-P2] with the SMC-B taking the place of the HPC towards a related PIN sending card, i.e. an SMC-A. For this purpose, RSA authentication with storage of introduction keys is set as algorithm in the SMC-B.

6.9.6 Symmetric Authentication as PIN Sender

If a certain SMC-B and a certain RFID Token have been introduced to each other before, i.e. had performed an asymmetric authentication including the persistent storage of introduction keys, then both cards can perform a symmetric authentication by using the shared introduction keys. The procedure is performed as described in Clause 5.9.4. For this purpose, DES authentication with agreement on session keys for trusted channel is set as algorithm in the SMC-B.

6.9.7 Symmetric Authentication as PIN Receiver

If a certain SMC-B and a certain SMC-A have been introduced to each other before, i.e. had performed an asymmetric authentication including the persistent storage of introduction keys, then both cards by using the shared introduction keys can perform a symmetric authentication. The procedure is performed as described in Clause 7.5 of [HPC-P2] with the SMC-B taking the place of the HPC. For this purpose, DES authentication with agreement on session keys for secure messaging is set as algorithm in the SMC-B.

6.10 The Security Module Application

6.10.1 File Structure and File Content

The file structure of DF.SMA for SMC-B is shown in the subsequent Figure.

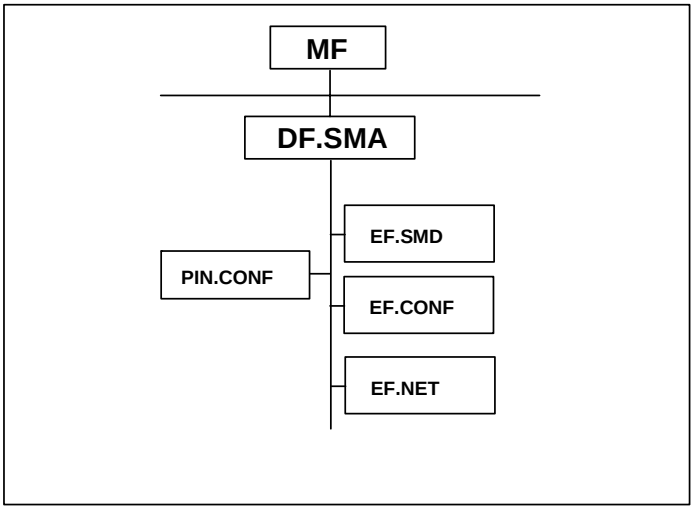

Figure 6 – (N3512.00) General structure of the SMA application in SMC-B

6.10.2 DF.SMA (Security Module Application)

DF.SMA is an application according to Clause 8.3.1.1 of [HPC-P1], i.e. selectable by using the application identifier. Table 106 (N3513.00) shows the characteristics of the application directory.

Table 106 – (N3513.00) Characteristics of MF / DF.SMA

Attribute	Value	Note
Object type	Application Directory	
Application Identifier	'D27600014607'	
File Identifier	-	Manufacturer-specific; if supported, then out of interval ['1000', 'FEFF']; see Clause 8.1.1 of [HPC-P1]
Life Cycle Status	Operational state (activated)	
Access Rule in all SEs		
Access Mode	**Security Condition**	**Note**
SELECT	ALWAYS	
LOAD APPLICATION (after SMC-B issuing)	AUT('D27600014600' || '01') AND SmMac AND SmCmdEnc	Only executable if a CAMS is used; see 5.12. If a CAMS with symmetric authentication is used, then the security condition must contain the key reference of the corresponding symmetric key, i.e. AUT('13') instead of AUT('D27600014600' || '01').
ACTIVATE, DEACTIVATE, DELETE	NEVER	

6.10.2.1 EF.SMD

The usage of EF.SMD is the same as for SMC-A; see Clause 5.10.1.2. The access conditions specified in Table 107 (N3514.00) are slightly different from those on an SMC-A: the PIN.SMC can be used as alternative to the authentication of the related HPC or SMC for the updating or erasing access.

Table 107 – (N3514.00) Characteristics of MF / DF.SMA / EF.SMD

Attribute	**Value**	**Note**
Object type	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	...	
Access Rule in all SEs		
Access Mode	**Security Condition**	**Note**
SELECT, READ BINARY	ALWAYS	
UPDATE BINARY, ERASE BINARY	PWD(PIN.SMC) OR AUT('D27600004000' || 'xx')	Authentication with PIN.SMC or role authentication of HPC or SMC with related personal profile, e.g. profile 2; see [HPC-P2], Table (N2623.00)
ACTIVATE, DEACTIVATE, DELETE	NEVER	

6.10.2.2 EF.CONF

The transparent file EF.CONF stores configuration data used for connector maintenance, useful e.g. during exchange of connectors to back up and transfer pairing information to the new connector. Reading, updating and erasing data is only allowed after successful presentation of PIN.CONF.

The access conditions and other characteristics of EF.CONF are specified in Table 108 (N3515.00).

Table 108 – (N3515.00) Characteristics of MF / DF.SMA / EF.CONF

Attribute	**Value**	**Note**
Object type	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	...	
Access Rule in all SEs		
Access Mode	**Security Condition**	**Note**
SELECT	ALWAYS	
READ BINARY, UPDATE BINARY, ERASE BINARY	PWD(PIN.CONF)	Authentication with PIN.CONF; see Table 110 (N3517.00)
ACTIVATE, DEACTIVATE, DELETE	NEVER	

6.10.2.3 EF.NET

The transparent file EF.NET may be used for storing net configuration data with less need for protection than data in EF.CONF, e.g.

- DNS-names or IP addresses in combination with port number and protocol type (TCP or UDP) of the access gateways
- VPN IP-version (IPv4 or IPv6)
- DNS-name of the update server.

The data are organizational unit specific. It is always allowed to read the data. Updating and erasing is only allowed after successful presentation of PIN.SMC. The access conditions and further characteristics of EF.NET are specified in Table 109 (N3516.00).

Table 109 – (N3516.00) Characteristics of MF / DF.SMA / EF.NET

Attribute	**Value**	**Note**
Object type	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	...	
Access Rule in all SEs		
Access Mode	**Security Condition**	**Note**
SELECT, READ BINARY	ALWAYS	
UPDATE BINARY, ERASE BINARY	PWD(PIN.SMC)	The access rule for PIN.SMC is specified at MF level.
ACTIVATE, DEACTIVATE, DELETE	NEVER	

6.10.2.4 PIN.CONF

PIN.CONF is a local PIN for writing and reading access to the configuration data in EF.CONF. The PIN consists of 6 to 8 digits and is changeable. The retry counter shall have the initial value 3.

The usage of the 8 digit resetting codes (personal unblocking key, PUK) is limited by a usage counter with an initial value of 10. The usage counter is decremented irrespective of whether the resetting code was correct or not. The successful presentation resets the retry counter of the related PIN.CONF. The security status of PIN.CONF can be used an unlimited number of times, i.e. the default number of SSEC is set to infinite. The attributes and access rules of PIN.CONF are shown in the following table.

Table 110 – (N3517.00) Characteristics of MF / DF.SMA / PIN.CONF

Attribute	**Value**	**Note**
Object type	Password	
Password Identifier	'01'	
Password Reference	'81'	
Secret	....	To be personalized
Minimum Length	6	
Start Retry Counter	3	
Retry Counter	3	
Transport Status	One of the methods given in Clause 8.2.5 of [HPC-P1]	
Flag Enabled	True	
Start Security Status Evaluation Counter	Infinite	
PUK	...	To be personalized
PUK Usage	10	

Access Rule in all SEs		
Access Mode	**Security Condition**	**Note**
CHANGE RD (Option ‘00’)	ALWAYS	
GET PIN STATUS	ALWAYS	
RESET RC (Option ‘00’ and ‘01’)	ALWAYS	
VERIFY	ALWAYS	
Other	NEVER	

According to Clause 14.6.1.4 and Clause 14.6.5.6 of [HPC-P1] the COS checks only the minimum length (6 digits) of PIN.CONF, i.e. the COS does not control whether the maximum length of 8 digits is exceeded.

The method for PIN transport protection shall be one given in Clause 8.2.5 of [HPC-P1]. It is recommended to use an empty-PIN method that simply demands the entry of the new PIN from the user. The command CHANGE REFERENCE DATA is used to establish the regular PIN; see Clause 4.6.2 of [HPC-P2].

The PIN management functions are the same as for PIN.CH of the HPC; see Clause 4.6 of [HPC-P2].

6.10.3 Application Selection

The application selection is performed with the ISO/IEC 7816-4 SELECT command as shown in the subsequent two tables.

Table 111 - (N3518.00) SELECT command for DF.SMA

CLA	As defined in ISO/IEC 7816-4
INS	‘A4’ = SELECT
P1	‘04’ = DF selection by AID
P2	‘0C’ = No FCI to return
Lc	‘06’ = Length of subsequent data field
Data field	‘D27600014607’ = AID of DF.SMA of SMC-B
Le	Absent

Table 112 - (N3519.00) SELECT response

Data field	Absent
SW1-SW2	‘9000’ or specific status bytes; see [HPC-P1]

6.10.4 Reading, Updating and Erasing Data of EF.SMD, EF.CONF and EF.NET

For reading, updating and erasing data of EF.SMD, EF.CONF and EF.NET the same commands are used as described in Clause 5.10.4.

6.11 The ESIGN Application

6.11.1 File Structure and File Content

DF.ESIGN is used for

- organizational signature computation (signature is bound to the respective health care institution and not to a single person; see Figure 7 (N3520.00)),
- client-server authentication e.g. for connecting a health care institution or a part of it to the health care VPN, and
- key decipherment and key transcipherment for confidential transfer of documents addressed to the respective health care institution and not to a single person.

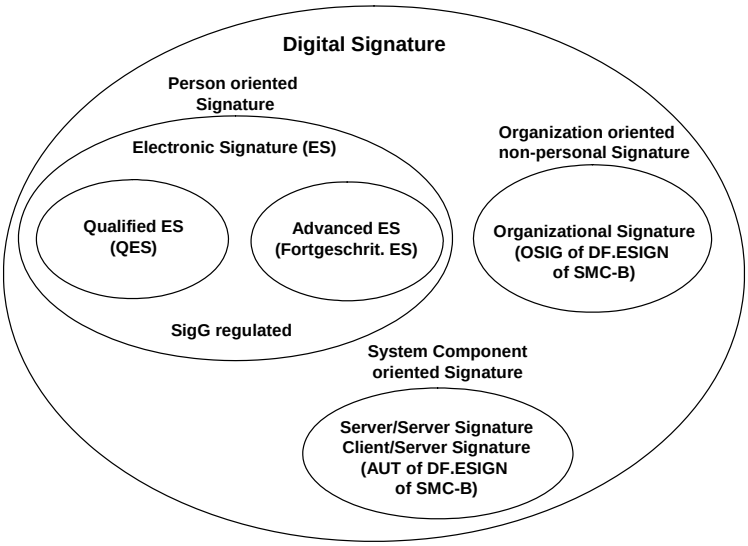

Figure 7 – (N3520.00) Digital Signature Types

The general file structure of the ESIGN application, which is in accordance with EN14890, is shown in Figure 8 (N3521.00).

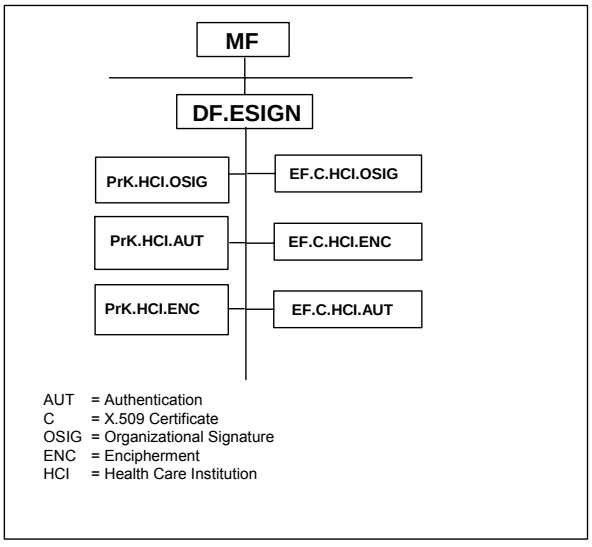

Figure 8 – (N3521.00) General structure of DF.ESIGN

6.11.2 DF.ESIGN (ESIGN Application)

DF.ESIGN is an application according to Clause 8.3.1.1 of [HPC-P1], i.e. selectable by using the application identifier. Table 113 (N3522.00) shows the characteristics of the application directory.

Table 113 – (N3522.00) Characteristics of MF / DF.ESIGN

Attribute	Value	Note
Object type	Application Directory	
Application Identifier	'A000000167 455349474E'	
File Identifier	-	Manufacturer-specific; if supported, then out of interval [‘1000’, ‘FEFF’]; see Clause 8.1.1 of [HPC-P1]
Life Cycle Status	Operational state (activated)	
Access Rule in all SEs		
Access Mode	**Security Condition**	**Note**
SELECT	ALWAYS	
LOAD APPLICATION, ACTIVATE, DEACTIVATE, DELETE	NEVER	

6.11.3 EF.C.HCI.OSIG

EF.C.HCI.OSIG contains the X.509 certificate for the organizational signature function of the SMC-B. The characteristics of the certificate file are shown in Table 114 (N3523.00).

Table 114 – (N3523.00) Characteristics of MF / DF.ESIGN / EF.C.HCI.OSIG

Attribute	Value	Note
Object type	Transparent Elementary File	
File Identifier	‘C000’	
Short File Identifier	‘10’ = 16	
Number of Bytes	1536 or limited to length of certificate	
Flag Transaction Mode	False	
Flag Checksum	False	
Life Cycle Status	Operational state (activated)	
Content	...	To be personalized.
Access Rule in all SEs		
Access Mode	**Security Condition**	**Note**
SELECT, READ BINARY	ALWAYS	
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, UPDATE BINARY	NEVER	

6.11.4 EF.C.HCI.AUT

EF.C.HCI.AUT contains the X.509 certificate for the client/server authentication service of the SMC-B. The characteristics of the certificate file are shown in Table 115 (N3524.00).

Table 115 – (N3524.00) Characteristics of MF / DF.ESIGN / EF.C.HCI.AUT

Attribute	Value	Note
Object type	Transparent Elementary File	
File Identifier	‘C500’	
Short File Identifier	‘01’ = 1	

Number of Bytes	1536 or limited to length of certificate	
Flag Transaction Mode	False	
Flag Checksum	False	
Life Cycle Status	Operational state (activated)	
Content	...	To be personalized.
Access Rule in all SEs		
Access Mode	**Security Condition**	**Note**
SELECT, READ BINARY	ALWAYS	
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, UPDATE BINARY	NEVER	

6.11.5 EF.C.HCI.ENC

EF.C.HCI.ENC contains the X.509 certificate for the service of deciphering and transciphering enciphered documents which were addressed to the health care institution and not to a single person. The characteristics of the certificate file are shown in Table 116 (N3525.00).

Table 116 – (N3525.00) Characteristics of MF / DF.ESIGN / EF.C.HCI.ENC

Attribute	**Value**	**Note**
Object type	Transparent Elementary File	
File Identifier	'C200'	
Short File Identifier	'02' = 2	
Number of Bytes	1024 or limited to length of certificate	
Flag Transaction Mode	False	
Flag Checksum	False	
Life Cycle Status	Operational state (activated)	
Content	...	To be personalized.
Access Rule in all SEs		
Access Mode	**Security Condition**	**Note**
SELECT, READ BINARY	ALWAYS	
ACTIVATE, DEACTIVATE, DELETE, ERASE BINARY, UPDATE BINARY	NEVER	

6.11.6 PrK.HCI.OSIG

PrK.HCI.OSIG is the private key for the PKI service of organizational signature computation. The key characteristics are shown in the subsequent table.

Table 117 – (N3526.00) Characteristics of MF / DF.ESIGN / PrK.HCI.OSIG

Attribute	**Value**	**Note**
Object type	Private RSA Object	
Key Identifier	'04' = 4	
Key Reference	'84'	
Private Key	.... (2048 bit)	To be personalized
Key Available	True	
Algorithm Identifier	signPKCS1_V1_5 signPSS sign9796_2_DS2	
Access Rule in SE # 1		
Access Mode	**Security Condition**	**Note**
COMPUTE DIGITAL SIGNATURE (P2 = '9E' or 'AC')	PWD(PIN.SMC)	The access rule for PIN.SMC is specified at MF level.
Other	NEVER	

The length of the key is compliant with the key length recommended by the end of 2013 for qualified electronic signatures [TR-03116].

6.11.7 PrK.HCI.AUT

PrK.HCI.AUT is the private key for the PKI service of client-server authentication. The key characteristics are shown in the subsequent table.

Table 118 – (N3527.00) Characteristics of MF / DF.ESIGN / PrK.HCI.AUT

Attribute	Value	Note
Object type	Private RSA Object	
Key Identifier	'02' = 2	
Key Reference	'82'	
Private Key	.... (2048 bit)	To be personalized
Key Available	True	
Algorithm Identifier	INTERNAL AUTHENTICATE: rsaClientAuthentication PSO: COMPUTE DIGITAL SIGNATURE: signPKCS1_V1_5 signPSS sign9796_2_DS2	
Access Rule in all SEs		
Access Mode	**Security Condition**	**Note**
INTERNAL AUTHENTICATE, COMPUTE DIGITAL SIGNATURE (P2 = '9E' or 'AC')	PWD(PIN.SMC)	The access rule for PIN.SMC is specified at MF level.
Other	NEVER	

The length of the key is compliant with the key length recommended by the end of 2013 for client/server authentication [TR-03116].

6.11.8 PrK.HCI.ENC

PrK.HCI.ENC is the private key for the PKI service of key decipherment and key transcipherment. The key characteristics are shown in the subsequent table.

Table 119 – (N3528.00) Characteristics of MF / DF.ESIGN / PrK.HCI.ENC

Attribute	Value	Note
Object type	Private RSA Object	
Key Identifier	'03' = 3	
Key Reference	'83'	
Private Key	.... (2048 bit)	To be personalized
Key Available	True	
Algorithm Identifier	rsaDecipherOaep rsaDecipherPKCS1_V1_5	
Access Rule in all SEs		
Access Mode	**Security Condition**	**Note**
PSO: DECIPHER, PSO: TRANSCIPHER	PWD(PIN.SMC)	The access rule for PIN.SMC is specified at MF level.
Other	NEVER	

The length of the key is compliant with the key length recommended by the end of 2013 for encryption [TR-03116].

6.11.9 Reading the X.509 Certificates

The reading of X.509 certificates is described in Clause 10.4 of [HPC-P2].

6.11.10 Using the Private Keys

Prior to the usage of any of the private keys, PIN.SMC has to be successfully presented.

For calculation of an electronic signature with the PSO: COMPUTE DIGITAL SIGNATURE command, the same command sequence as described in Clause 9.8 of [HPC-P2] is applied.

The client/server authentication is performed as described in Clause 10.6 of [HPC-P2].

The deciphering of a document encipher key with the PSO: DECIPHER command is specified in Clause 10.7 of [HPC-P2].

The transciphering of a document encipher key with the PSO: TRANSCIPHER command is specified in Clause 10.8 of [HPC-P2].

6.12 The Card Terminal Application

The characteristics and usage of DF.KT are the same as for SMC-A; see Clause 5.11.

6.13 Loading a new Application or Creation of an EF after SMC-B Issuing

It is assumed that the loading of a new application on MF level (including updating the files EF.DIR and EF.Version) or the creation of a new EF in DF.SMA after issuing of the SMC-B is performed by a Card Application Management System (CAMS). This is an optional procedure.

Similarly, a CAMS is optional. The content of Chapter 13 of [HPC-P2] is however normative, if loading of a new application or creation of a new EF after SMC-B issuing are to be performed.