Specification

German
Health Professional Card
and
Security Module Card

Part 3: SMC Applications and Functions

Version 2.1.0

21.02.2006

BundesÄrzteKammer

Kassenärztliche Bundesvereinigung

BundesZahnÄrzteKammer

BundesPsychotherapeutenKammer

Kassenzahnärztliche Bundesvereinigung

Werbe- und Vertriebsgesellschaft Deutscher Apotheker mbH

Deutsche Krankenhaus-Gesellschaft

Zentralinstitut für die kassenärztliche Versorgung in der BRD

Editor: Bruno Struif, 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

Contents

1 Scope

This part of the specification defines the card interface to

- the Security Module Card (SMC) designed for use in health institutions.

The SMC provides services such as

- C2C authentication SMC/eGK
- trusted channel support allowing the usage of remote HPCs and electronic Health Cards
- 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.

The SMC may be used in card terminals as well as in connector systems.

2 References

[ALGCAT]
Geeignete Algorithmen zur Erfüllung der Anforderungen nach §17 Abs. 1 bis 3 SigG vom 22. Mai 2001 in Verbindung mit Anlage 1 Abschnitt I Nr. 2 SigV vom 22. November 2001, 30. März 2005, Bundesanzeiger Nr. 59, S. 4695-4696
See also www.bundesnetzagentur.de

[BÄK-HBA-Ausgabe]
Bundesärztekammer
Ausgabe Heilberufsausweis (HBA)
Fachfeinkonzept

[BÄK-HBA-Lastenheft]
Bundesärztekammer
Lastenheft zur Spezifikation der HPC/SMC

[CWA14890-1]
“eSIGN Specification”
Application Interface for SmartCards used as Secure Signature Creation Devices
Part 1 – Basic Requierements
March 8th 2004

[CWA14890-2]
”eSIGN Specification”
Application Interface for SmartCards used as Secure Signature Creation Devices
Part 2 – Additional services
March 12th 2004

[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
Die Spezifikation der elektronischen Gesundheitskarte
Teil 1 – Kommandos, Algorithmen und Funktionen der Betriebssystem-Plattform
V1.1.0, 07.02.2006

[eGK-P2]
gematik
Die Spezifikation der elektronischen Gesundheitskarte
Teil 2 – Anwendungen und anwendungsspezifische Strukturen
V1.1.0, 07.02.2006

[EN1867]
prEN 1867: 1995
Machine readable cards - Health care applications - Numbering system and registration procedure for issuer identifiers

[HPC-P1]
German Health Professional Card and Security Module Card
Part 1: Commands, Algorithms and Functions of the COS Platform
V2.1.0, 21.02.2006

[HPC-P2]
German Health Professional Card and Security Module Card
Part 2: HPC Applications and Functions
V2.1.0, 21.02.2006

[ISIS-MTT OP]
T7, TeleTrusT: ISIS-MTT Specification, Optional Profile "SigG-Profile", Version 1.1, 16th March 2004, www.teletrust.de

[ISIS-MTT P1]
T7, TeleTrusT: ISIS-MTT Specification, Part 1 "Certificate and CRL Profiles", Version 1.1, 16th March 2004, www.teletrust.de

[ISO3166]
ISO/IEC 3166: Codes for the representations of names of countries

[ISO7812]
ISO/IEC 7812-1:2000
Identification cards – Identification of issuers – Part 1: Numbering system

[ISO7816-1]
ISO/IEC 7816-1: 1996 (2nd edition)
Identification cards - Integrated circuit cards with contacts -
Part 1: Physical characteristics

[ISO7816-2]
ISO/IEC 7816-2: 1996 (2nd edition)
Identification cards - Integrated circuit cards with contacts -
Part 2: Dimensions and location of contacts

[ISO7816-3]
ISO/IEC 7816-3: FCD2 2005 (2nd edition)
Identification cards - Integrated circuit cards with contacts -
Part 3: Electrical interface and transmission protocols

[ISO7816-4]
ISO/IEC 7816-4: 2005 (2nd edition)
Identification cards - Integrated circuit cards -
Part 4: Organization, security and commands for interchange

[ISO7816-5]
ISO/IEC 7816-5: 2004 (2nd edition)
Identification cards - Integrated circuit cards -
Part 5: Registration of application providers

[ISO7816-6]
ISO/IEC 7816-6: 2004 (2nd edition)
Identification cards - Integrated circuit cards -
Part 6: Interindustry data elements for interchange

[ISO7816-8]
ISO/IEC 7816-8: 2004 (2nd edition)
Identification cards - Integrated circuit cards -
Part 8: Commands for security operations

[ISO7816-9]
ISO/IEC 7816-9: 2004 (2nd edition)
Identification cards - Integrated circuit cards -
Part 9: Commands for card management

[ISO7816-13]
ISO/IEC 7816-13: CD2 2005
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: 1995
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, Banking – Personal Identification Number management and Security -
Part 1: PIN protection principles and techniques, 1999

[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

[ISO10918]
ISO/IEC 10918-1: 1994
Information technology - digital compression and coding of continuous-tone still images: Requirements and guidelines

[ISO11770]
ISO/IEC 11770: 1996
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 vesions: V1.5: Nov. 1993, V2.0: July, 1998)

[PP-SMC]
Common Criteria Protection Profile – Security Module Card (SMC)

[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

[RFC2279]
UTF-8, a transformation format of ISO 10646, January 1998

[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

[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

[SSL]
Netscape:
SSL3.0 Specification

3 Abbreviations and Notations

3.1 Abbreviations

AC = Attribute Certificate
AID = Application Identifier
AM = Access Mode
AOD = Authentication Object Directory
ARR = Access Rule Reference
ASIG = Advanced electronic Signatures
ASN.1 = Abstract Syntax Notation One
AT = Authentication Template
ATR = Answer-to-Reset
AUT = Authentication
AVS = Apothekenverwaltungssystem
BCD = Binary Coded Decimal
BÄK = Bundesärztekammer
BER = Basic Encoding Rules
BNA = BundesNetzAgentur
C = Certificate
CAMS = Card Application Management System
C2C = Card-to-Card
CA = Certification Authority
CAR = Certification Authority Reference
CBC = Cipher Block Chaining
CC = Cryptographic Checksum
CD = Certificate Directory
CE = Certificate Extensions
CG = Cryptogram
CH = Cardholder
CHA = Certificate Holder Authorization
CHR = Certificate Holder Reference
CIA = Cryptographic Inform. Application
CIO = Cryptographic Inform. Objects
CLA = Class byte of a command
COS = Card Operating System
CPI = Certificate Profile Identifier
CRT = Control Reference Template
CS = CertSign (= CertificateSigning)
CT = Confidentiality Template
CVC = Card Verifiable Certificate
CWA = CEN Working Agreement
D, DIR = Directory
DE = Data Element
DER = Distinguished Encoding Rules
DES = Data Encryption Standard
DO = Data Object
DF = Dedicated File
DI = Baud rate adjustment factor
DNS = Domain Name Service
DSI = Digital Signature Input
DST = Digital Signature Template
E = Evaluation
EAL = Evaluation Assurance Level
EF = Elementary File
eGK = elektronische Gesundheitskarte (electronic Health Card)
ENC = Encipherment
EOF = End-of-File
FCI = File Control Information
FI = Clock rate conversion factor
FID = File Identifier
FM = File Management
HB = Historical Bytes
HF2 = Hash Function ISO 10118-2
HCI = Health Care Institution
HP = Health Professional
HPC = Health Professional Card
ICC = Integrated Circuit Card

ICCSN = ICC Serial Number
ID = Identifier
IFD = Interface Device
IFSC = Information Field Size Card
IFSD = Information Field Size Device
IIN = Issuer Identification Number
IK = Individual Key
IP = Internet Protocol
IV = Initial Value
KD = Key Derivation data
KE = Key Encipherment
KEI = Key Encipherment Input
KID = Key Identifier
LSB = Least Significant Byte(s)
MF = Master File
MII = Major Industry Identifier
MSE = MANAGE SECURITY ENVIRONMENT
OID = Object Identifier
OSIG = Organizational Signature
P = Patient
PHAR = Pharmacist
PHYS = Physician
PK,PuK = Public Key
PI = Padding Indicator
PIN = Personal Identification Number
PIX = Proprietary Appl. Prov. Extension
PP = Protection Profile
PPS = Protocol Parameter Selection
PrK = Private Key
PRND = Padding Random Number
PSO = PERFORM SECURITY OPERATION
PUK = Personal Unblocking Key (= Resetting Code)
PVS = Praxis-Verwaltungssystem
R = Role ID
RC = Retry Counter
RCA = Root CA
RD = Reference Data
RFC = Request for Comment
RID = Registered Application Provider Id.
RND = Random Number
RSA = Algorithm of Rivest, Shamir, Adleman
S = Server
SC = Security Condition
SFID = Short EF Identifier
SIG = Signature
SK = Secret Key
SM = Secure Messaging
SMA = Security Module Application
SMC = Security Module Card
SMD = SMC related Data
SMK = SM Key
SSC = Send Sequence Counter
SSCD = Secure Signature Creation Device
SSL = Security Sockets Layer
SN = Serial Number
TC = Trusted Channel
TCP = Transmission Control Protocol
TLS = Transport Layer Security
UDP = User Datagram Protocol
UID = User Identification
UQ = Usage Qualifier
VD = Verification Data
VPN = Virtual Private Network
ZGW = CA for heath care (Zertifizierungsstelle Gesundheitswesen)

3.2 Notations

For keys and certificates the following simplified Backus-Naur notation applies:

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

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

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

<private key>::= PrK (asym.)
<public key>::= PuK (asym.)
<secret key>::= SK (sym., not used)
<individual key>::= IK (sym., not used)

<keyholder>::= <health professional> | <card holder> | <certification authority> | <health professional card> | <electronic health card> | <security module card> | <server>

<health professional> ::= HP
<card holder> ::= CH
<certification authority >::= RCA | CA | CA_NN
<health professional card> ::= HPC
<electronic health card> ::= eGK (elektronische Gesundheitskarte)
<security module card> ::= SMC
<server> ::= S

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

< organizational signature>::= OSIG
<encipherment >::= ENC
<authentication>::= AUT
<certsign>::= CS

<SMkey> ::= SMK.ENC | SMK.MAC

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

<certificate>::= <X.509v3 certificate> | <card verifiable certificate>
<X.509v3 certificate>::= C
<card verifiable certificate>:: CVC

<certificate holder>::=
<health professional> | <certification authority> | <health professional card> | <security module card> | <server>

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

<organizational signature>::= OSIG
<encipherment>::= ENC
<authentication>::= AUT
<certsign>::= CS

For subsequent data items the following notation is used:

|| = Concatenation of data

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

4 Technical Characteristics, Answer-to-Reset and Transmission Protocols

For the SMC the same conventions apply for the technical characteristics, Answer-to-Reset and transmission protocols as for the HPC, see [HPC-P1]. The SMC is designed for use as plug-in card present in related card terminals or connectors.

5 Security Module Cards

5.1 General Structure

A SMC provides similar functions as a 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 – SMC Types

SMC Type	Configuration	Usage	Application Scenario
A	- CVC authentication procedure and secure command processing for trusted channel support - no PKI keys and X.509 certificates	- eGK/SMC authentication after SMC authorization through a HPC - HPC/SMC authentication with trusted channel establishment for remote HPC handling	Used e.g. in card terminals (referred as "Arbeitsplatzkarte")
B	- Functionality of type A - EF.NET for net configuration data - PKI keys for OSIG, ENC & AUT and related X.509 certificates (no attribute certificates)	- eGK/SMC authentication after SMC authorization through a HPC - HPC/SMC authentication with trusted channel establishment for remote HPC handling - provision of net configuration data PKI services for the respective HCI: - Deciphering of enciphered documents addressed to the HCI and not to a single person - client/server authentication - advanced signature function	Used e.g. once per organizational entity in a connector (referred as "Institutionenkarte")

5.2 Logical Channels

SMCs support at least 4 logical channels.The channel management shall be performed as specified in [HPC-P2].

6 SMC Type A

6.1 General Structure

The general structure of SMC Type A is shown in Figure 1.

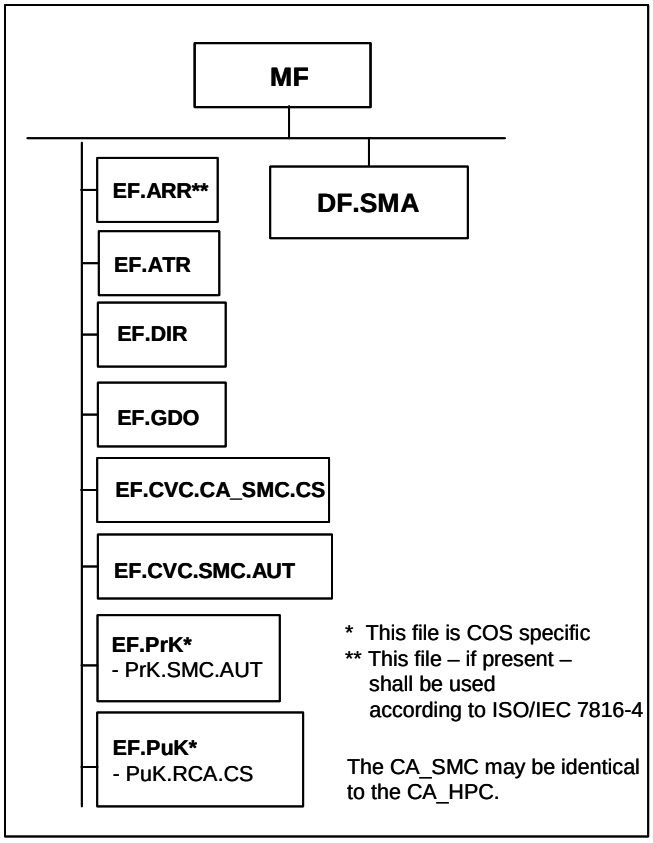

Figure 1 – General file structure of a SMC

NOTE – For SMC Type A no PIN is necessary, since the usage of the private key PrK.SMC.AUT depends on the successful authorization of a related HPC.

6.2 CVC Key Management Authorities

Asymmetric authentication procedures with CV certificates are supported in the SMC for

- proving access rights to an electronic health card (eGK) after the respective security status is reached through external authentication of a related HPC
- verification of the authenticity of an eGK
- support of trusted channel between HPC and SMC or eGK and SMC.

The general model for CV Certificates and CVC Key Management Authorities is shown in [HPC-P2].

For CVC verification, a SMC contains

- the public key of the Root CA: PuK.RCA.CS.

6.3 Elementary Files at MF-Level

6.3.1 EF.ARR

EF.ARR contains the access rules relevant at MF level.

6.3.2 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'. The content of EF.ATR is specified in Table B.1.

6.3.3 EF.DIR

EF.DIR contains the application template for DF.SMA. The content of EF.DIR is specified in Table B.4.

6.3.4 EF.GDO

EF.GDO contains in compliance with [Resolution190] the DO ICC Serial Number (ICCSN, Tag '5A', see Figure 2).

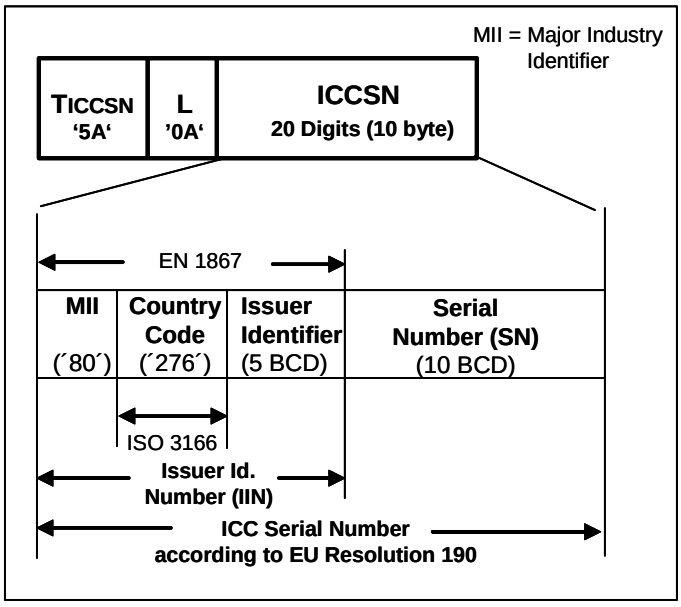

Figure 2 - ICC Serial No. for health cards

Only a registered IIN is allowed as part of the ICCSN, see Annex H 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).

6.3.5 EF.CVC.CA_SMC.CS

EF.CVC.CA_SMC.CS contains the card verifiable certificate of the Certificate Service Provider, issued by the Root CA for Health Care. The CA_SMC is possibly the same as the CA_HPC. Structure and content of the CVC are outlined in [HPC-P1].

6.3.6 EF.CVC.SMC.AUT

EF.CVC.SMC.AUT contains the card verifiable certificate of the SMC for card-to-card authentications between eGK and SMC. Structure and content of the CVC are outlined in [HPC-P1].

The Certificate Holder Authorizations relevant for a CVC.SMC.AUT are shown in Table A.3.

6.3.7 EF.PrK

EF.PrK contains

- the global private key PrK.SMC.AUT for C2C-authentication (SMC/HPC and SMC/eGK).

The key characteristics are shown in Table 2.

Table 2 – Key characteristics

Key Name	Key length	KeyID	SE #	Access Conditions
PrK.SMC.AUT (for SMC/eGK authentication without TC establishment)	1024 bit (RSA)	'10' see note	'01'	Ext. Authentication of related HPC, see Annex A
PrK.SMC.AUT (for SMC/HPC and SMC/eGK authentication with TC establishment)	1024 bit (RSA)	'11' see note	'02'	Ext. Authentication of related HPC, see Annex A

NOTE - In cards supporting multi-KID-referencing of a key object (i.e. the same key has more than one KID), the key is only present once. In other cards the key may be stored twice. The purpose of the key is bound to the KID. Therefore the AlgID is implicit.

The public key associated with PrK.SMC.AUT is contained in CVC.SMC.AUT.

6.3.8 EF.PuK

EF.PuK contains

- the public key PuK.RCA.CS of the Root CA for verification of CVCs issued by this RCA.

6.4 Security Environments at MF Level

At MF level the following SEs are used:

- SE # 1 is the general SE at MF level and used for all purposes except the one dedicated to SE # 2.
- SE # 2 is dedicated to the usage of PrK.SMC.AUT for trusted channel establishment between HPC and SMC or eGK and SMC (TC used e.g. for electronic prescription processing over internet).

6.5 SMC Opening

6.5.1 Reading of EF.ATR and EF.GDO

For reading EF.ATR and EF.GDO, the READ BINARY command is used, see [HPC-P2], Clause 5.6.2. Since the SMC remains in the respective device, this command is possibly performed only once.

6.5.2 Reading EF.DIR

For reading EF.DIR, the READ RECORD command is used, see [HPC-P2], Clause 5.6.3. Since the SMC remains in the respective device, this command is possibly performed only once.

6.5.3 Reading SMC related CV Certificates

For reading SMC related CV Certificates, the READ BINARY command is used, see [HPC-P2], Clause 5.6.4. Since the SMC remains in the respective device, this command is possibly performed only once by the software environment, e.g. PVS or AVS, which stores the CVCs e.g. associated with the respective ICCSN.SMC.

6.5.4 SE Selection at MF Level

If SE # 2 is necessary, the ISO/IEC 7816-4 MSE command (RESTORE function) has to be sent as specified in [HPC-P2].

6.6 Interactions between HPC and SMC

6.6.1 Establishment of a Trusted Channel and Handling of secured APDUs

This service requires the following actions at MF level:

- reading the CVCs of the SMC, see Clause 6.5.3
- selection of SE # 2 at MF level, see Clause 6.5.4.

6.6.1.1 Performing the Authentication Procedure

At first, CV certificates have to be exchanged and verified as described in [HPC-P2]. After that the authentication procedure with SM key agreement is performed as prescribed in [HPC-P1], Annex E.3, whereby the SMC is authenticated first.

The command sequence at the SMC side starts with selecting the involved keys.

Table 3 - MSE command for selecting the involved keys

CLA	As defined in ISO/IEC 7816-4
INS	‘22’ = MANAGE SECURITY ENVIRONMENT
P1	‘C1’ = SET for int./ext. authentication
P2	‘A4’ = AT
Lc	‘14’ = Length of subsequent data field
Data field	‘83 0C xx ... xx’ || ‘84 01 11’ = DO for KeyRef of PuK.HPC.AUT (for retrieval of the key reference, see Figure 3 in [HPC-P2]) || DO for KeyRef of PrK.SMC.AUT
Le	Absent

Table 4 - MSE response

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

After that the INTERNAL AUTHENTICATE command has to be sent to the SMC, containing the random no. retrieved from the HPC and the 8 LSB of the ICC Serial Number ICCSN8.HPC.

Table 5 - INT. AUTHENTICATE command

CLA	As defined in ISO/IEC 7816-4
INS	'88' = INTERNAL AUTHENTICATE
P1	'00'
P2	'00'
Lc	'10' = Length of subsequent data field
Data field	RND.HPC (8 byte) || ICCSN8.HPC (8 byte)
Le	'00' or 'xx' = length of expected signature

Table 6 - INT. AUTHENTICATE response

Data field	Authentication related data, see [HPC-P1], Annex E.3
SW1-SW2	'9000' or specific status bytes, see [HPC-P1]

Then a challenge is retrieved from the SMC.

Table 7 - 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 8 - GET CHALLENGE response

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

The challenge concatenated with ICCSN8.SMC will be sent to the HPC in the INTERNAL AUTHENTICATE command and the result is presented to the SMC with the EXTERNAL AUTHENTICATE command.

Table 9 - EXT. AUTHENTICATE command for HPC authentication

CLA	As defined in ISO/IEC 7816-4
INS	'82' = EXTERNAL AUTHENTICATE
P1	'00'
P2	'00'
Lc	'xx' = Length of subsequent data field
Data field	Authentication related data, see [HPC-P1], Annex E.3
Le	Absent

NOTE – The authentication related data contain DEs for SM key agreement.

Table 10 - EXT. AUTHENTICATE response

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

Upon successful authentication of the HPC, the security status "CHA.xx of HPC successfully presented" is set in the SMC.

The SM keys are computed as described in [HPC-P1], Annex E.3 and the initial value of the Send Sequence Counter is calculated as described in [HPC-P1], Annex C.5.2.

6.6.1.2 Production of secured Commands using PSO Commands

The usage of PSO commands for the production of secured commands is one possibility. The other possibility is the usage of the ENVELOPE command as speicifed in Clause 6.6.1.4. The indication which TC support method is supported, is indicated in the DO Card capabilities present in EF.ATR, see Annex B.1.

The general principles for TC support are shown in Annex D of [HPC-P1].

For the SM-DO production the following commands are used:

- PSO: COMPUTE CC
- PSO: ENCIPHER

Before, the SM keys for the PSO commands have to be set with MSE commands. All commands are sent in normal mode, since the SMC considers the the session keys as "user keys".

Table 11 - MSE command

CLA	As defined in ISO/IEC 7816-4
INS	‘22’ = MANAGE SECURITY ENVIRONMENT
P1	‘C1’ = SET for computation and verification
P2	‘B4’ = CCT
Lc	‘03’ = Length of subsequent data field
Data field	‘83 01 9E’ = DO for KeyID of SK.SMC.MAC
Le	Absent

Table 12 - MSE response

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

Table 13 - MSE command

CLA	As defined in ISO/IEC 7816-4
INS	‘22’ = MANAGE SECURITY ENVIRONMENT
P1	‘C1’ = SET for encipherment and decipherment
P2	‘B8’ = CT
Lc	‘03’ = Length of subsequent data field
Data field	‘83 01 9F’ = DO for KeyID of SK.SMC.ENC
Le	Absent

Table 14 - MSE response

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

Table 15 – PSO: COMPUTE CC command

CLA	As defined in ISO/IEC 7816-4
INS	‘2A’ = PSO: COMPUTE CC
P1	‘8E’ = CC in response data field
P2	‘80’ = PV in command data field
Lc	‘xx’ = Length of subsequent data field
Data field	Data for which the cryptographic checksum shall be computed (HPC command possibly with a DO PV, DO Le and a DO CG, see also note)
Le	'00'

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

Table 16 – PSO: COMPUTE CC response

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

If in the secured HPC command 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 send prior to the PSO: COMPUTE CC command.

Table 17 – PSO: ENCIPHER command

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

Table 18 – PSO: ENCIPHER response

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

6.6.1.3 Processing of secured Responses using PSO Commands

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

Table 19 – PSO: VERIFY CC command

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

Table 20 – PSO: VERIFY CC 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 21 – PSO: DECIPHER command

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

Table 22 – PSO: DECIPHER response

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

6.6.1.4 Production of secured Commands using the ENVELOPE Command

The stratgey in this case is to send as data the command to be secured to the SMC and to retrieve the cryptographic checksum DO and possibly also a cryptogram DO, so that the time consumption for producing a secured command is reduced. For this purpose, an ENVELOPE command with odd instruction code is send in normal mode to the SMC, i.e. the SMC considers the ENVELOPE command .

In the data field, the unsecured command in the DO Command-to-perform (tag '52') and an SM template (tag '7D') is present containg 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 23 – 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’ = Length of subsequent data field
Data field	- If the command to be secured contains data to be transmitted in DO PV (Case 1): '52'-L-command to be secured || '7D'-L-('BA' -L- ['8E'-'00']) - If the command to be secured contains data to be transmitted in a DO CG (Case 2): '52'-L-command to be secured || '7D'-L-('BA' -L- ['87'-'00' || '8E'-'00'])
Le	'00'

Table 24 – ENVELOPE response

Data field	- Case 1: '7D'-L-('8E' -'04'-CC) - Case 2: '7D'-L-('87' -L- '01'-CG || '8E' -'04'-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.

6.6.1.5 Processing of secured Responses using the ENVELOPE Command

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

- response with DO Processing status (tag '99')
- response with DO Plain value (tag '81')
- response with DO Cryptogram (tag '87').

All secured responses are protected by a cryptographic checksum CC.

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

The CC has to be verified. If a cryptogram is present, then the plain value has to be returned by the SMC after successful verification of the CC.

Table 25 – 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’ = 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'-'04'-CC) - Case 2 (Response APDU with DO Plain value and DO CC): '7D'-L-('81'-L- Data || '8E'-'04'-CC) - Case 3 (Response APDU with DO Cryptogram and DO CC): '7D'-L-('87' -L- '01'-CG || '8E'-'04'-CC || 'BA' -L- ['80'-'00'])
Le	Case 1, 2: Absent Case 3: '00'

Table 26 – ENVELOPE response

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

6.6.2 Authorization of a SMC by a HPC to interact with an eGK

According to [GMG], a health professional can authorize other dedicated persons to access an eGK using a SMC. The usage of the PrK.SMC.AUT for an SMC/eGK authentication procedure requires the successful authentication of an HPC, whereby the role ID present in the CHA of the CVC.HPC.AUT has to fit to the role ID present in the CHA of the CVC.SMC.AUT, see Annex A, Table A.3. The authentication procedure to be performed corresponds to that one described in [HPC-P1], Annex E.2, but only the HPC has to be authenticated. For import of the PuK.HPC.AUT,

- the CVC.CA_HPC.CS and
- the CVC.HPC.AUT

have to be verified by the SMC.

In a first step, the PuK.HPC.AUT has to be selected.

Table 27 - MSE command for selecting PuK.HPC.AUT

CLA	As defined in ISO/IEC 7816-4
INS	‘22’ = MANAGE SECURITY ENVIRONMENT
P1	‘81’ = SET for external authentication
P2	‘A4’ = AT
Lc	‘11’ = Length of subsequent data field
Data field	'83 0C xx ...' || ’80 01 1E’ = DO KeyRef of PuK.HPC.AUT (for retrieval of the key reference see Figure 3 in [HPC-P2]) || DO AlgID, see Table E.2 of [HPC-P2]
Le	Absent

Table 28 - MSE response

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

After that a challenge RND.SMC has to be retrieved from the SMC.

Table 29 - 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 30 - GET CHALLENGE response

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

The result of the INTERNAL AUTHENTICATE command performed by the HPC is then sent to the SMC in the EXTERNAL AUTHENTICATE command.

Table 31 - EXT. AUTHENTICATE command

CLA	As defined in ISO/IEC 7816-4
INS	‘82’ = EXTERNAL AUTHENTICATE
P1	‘00’
P2	‘00’
Lc	‘xx’ = Length of subsequent data field
Data field	Authentication related data, see [HPC-P1], Figure E.1
Le	Absent

Table 32 - EXT. AUTHENTICATE response

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

The digital signature will be verified by the SMC, which sets – if authentication successful – the security status required for the usage of the PrK.SMC.AUT for interactions with an eGK.

6.7 Interactions between eGK and SMC

6.7.1 SMC/eGK Authentication without TC Establishment

The SMC/eGK authentication is performed in the same way as the HPC/eGK authentication, see [HPC-P1] Annex E1.1, whereby the eGK is authenticated first.

6.7.2 SMC/eGK Authentication with TC Establishment

In the case that e.g. an electronic prescription shall be processed by an internet pharmacy, a trusted channel between an eGK and a SMC has to be established. The sequence of commands at the SMC interface after CVC verification is shown in [HPC-P1], Figure E.2. Prior to the performing of the authentication procedure

- SE # 2 has to selected and
- the keys involved have to be set as hown below.

Table 33 - MSE command for selecting the involved keys

CLA	As defined in ISO/IEC 7816-4
INS	'22' = MANAGE SECURITY ENVIRONMENT
P1	'C1' = SET for int./ext. authentication
P2	'A4' = AT
Lc	'11' = Length of subsequent data field
Data field	'83 0C xx ... xx' || '84 01 11' = DO for KeyRef of PuK.eGK.AUT (for retrieval of the key reference, see Figure 3 in [HPC-P2]) || DO for KeyRef of PrK.SMC.AUT
Le	Absent

Table 34 - MSE response

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

6.8 The Security Module Application SMA

6.8.1 File Structure and File Content

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

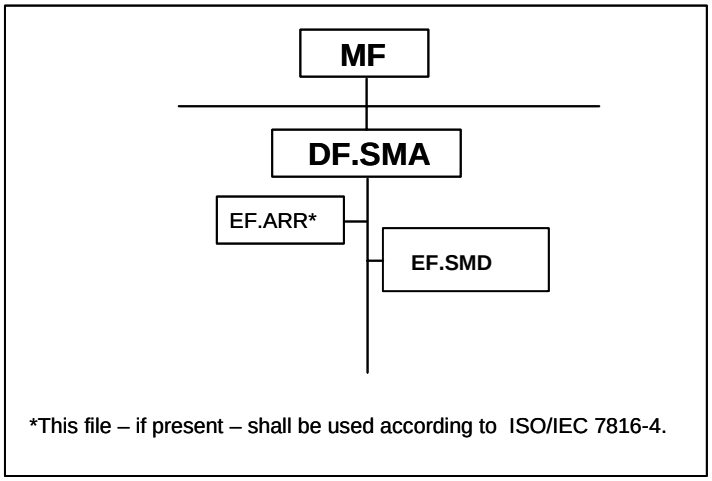

Figure 3 - File structure of DF.SMA in SMC Type A

In DF.SMA, only the default SE # 1 is used. For SMC Type A, no EF.NET is present under DF.SMA.

6.8.1.1 EF.ARR

EF.ARR contains the access rules related to DF.SMA.

6.8.1.2 EF.SMD

The transparent file EF.SMD is intended to be used for storing SMC related data, e.g. special configuration data. The file can be read always, but update is only possible after successful authentication of a related HPC.

6.8.2 Application Selection

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

Table 35 - 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	'D276 00004003' = AID of DF.SMA
Le	Absent

Table 36 - SELECT response

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

6.8.3 Reading and Updating of E.SMD

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

Table 37 - READ BINARY command for reading EF.SMD with SFID

CLA	As defined in ISO/IEC 7816-4
INS	'B0' = READ BINARY
P1	'81' = b8-b6: 100 b5-b1: 0001 SFID of EF.SMD: 1
P2	'00' = Offset
Lc	Absent
Data field	Absent
Le	'00' = Read until end-of-file

Table 38 - READ BINARY response

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

For updating EF.SMD the ISO/IEC 7816-4 command READ BINARY is used. The required security status for the udate operation is the successful presentation of a HPC with a related role ID, see Annex A.

Table 39 - UPDATE BINARY command for updating EF.SMD

CLA	As defined in ISO/IEC 7816-4
INS	‘D6’ = UPDATE BINARY
P1	'81' = b8-b6:100 b5-b1: 00001 SFID of EF.SMD: 1
P2	‘00’ = Offset
Lc	‘xx’ = Length of subsequent data field
Data field	Data
Le	Absent

Table 40 - UPDATE BINARY response

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

7 SMC Type B

7.1 General Structure

The general structure of SMC Type B is shown in Figure 4.

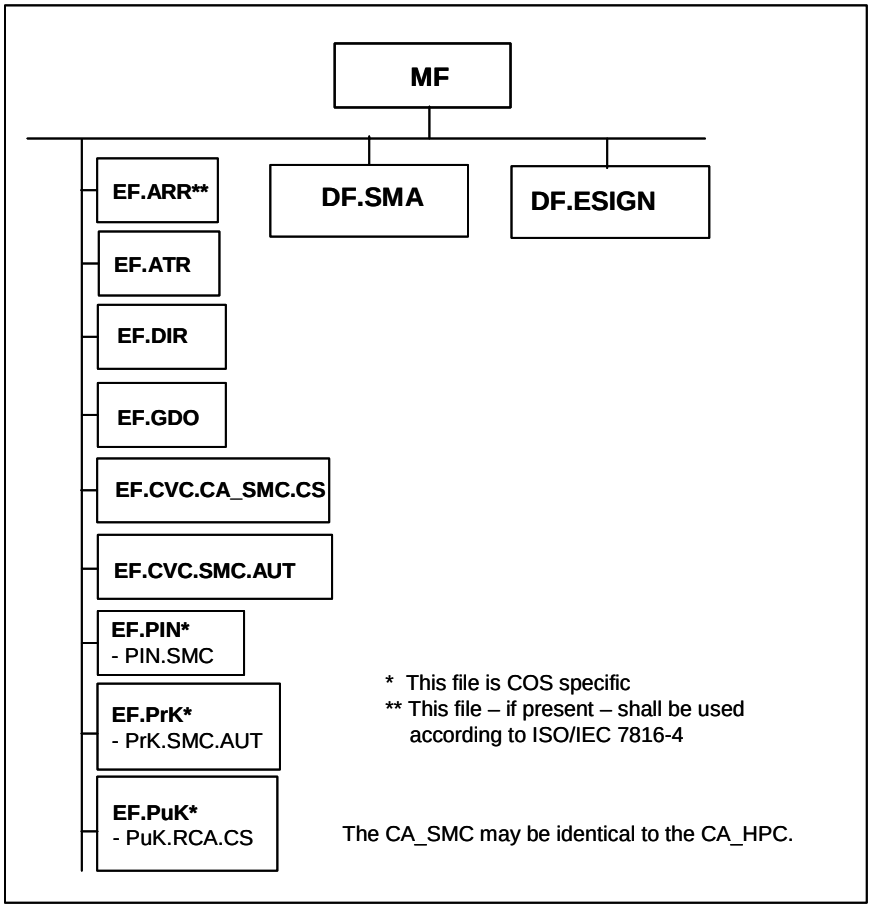

Figure 4 – General structure of the SMC Type B

The functionality of SMC Type B covers the full functionality of SMC Type A.

NOTE A cryptographic information application (DF.CIA.ESIGN) is not necessary, since a SMC remains stationary and the respective software knows the usage conventions.

7.2 Elementary Files at MF Level

7.2.1 EFs according to SMC Type B

All EFs of SMC Type A are are also present in SMC Type B, but additionally EF.PIN.

7.2.2 EF.PIN

EF.PIN contains the global PIN of the SMC Type B (PIN.SMC). The PIN characteristics are the same as for PIN.CH, see [HPC-P2].

7.3 The SMA Application

7.3.1 File Structure and File Content

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

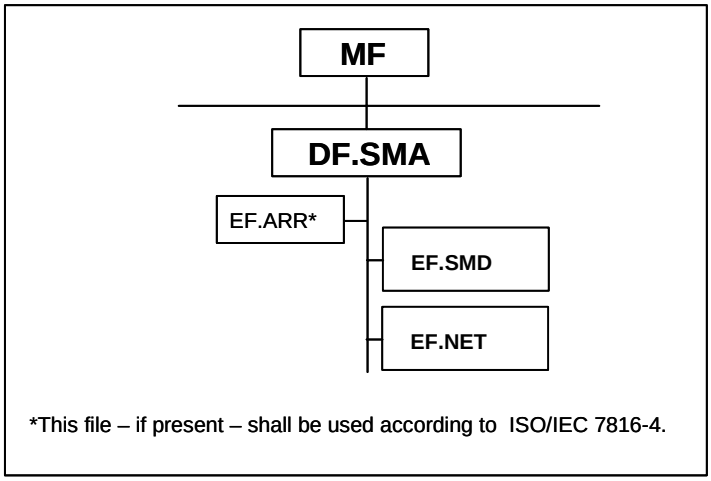

Figure 5 – General structure of the SMA application in SMC Type B

7.3.1.1 EF.SMD

The usage is the same as for SMC Type A, see Clause 6.8.1.2. The access conditions are specified in Annex A.

7.3.1.2 EF.NET

The transparent file EF.NET is used for storing net configuration data as used by a connector. The data are organizational unit specific (i.e. these data have to be provided for SMC personalization), see Clause B.6.

The access conditions for EF.NET are specified in Annex A.

7.3.2 Reading and Updating of EF.SMD and EF.NET

For reading and updating of EF.SMD and EF.NET the same commands as described in Clause 6.8.3 are used.

7.4 The ESIGN Application

7.4.1 General file structure and Usage

The general file structure of the ESIGN application, which is in accordance with [CWA14890], is shown in Figure 6.

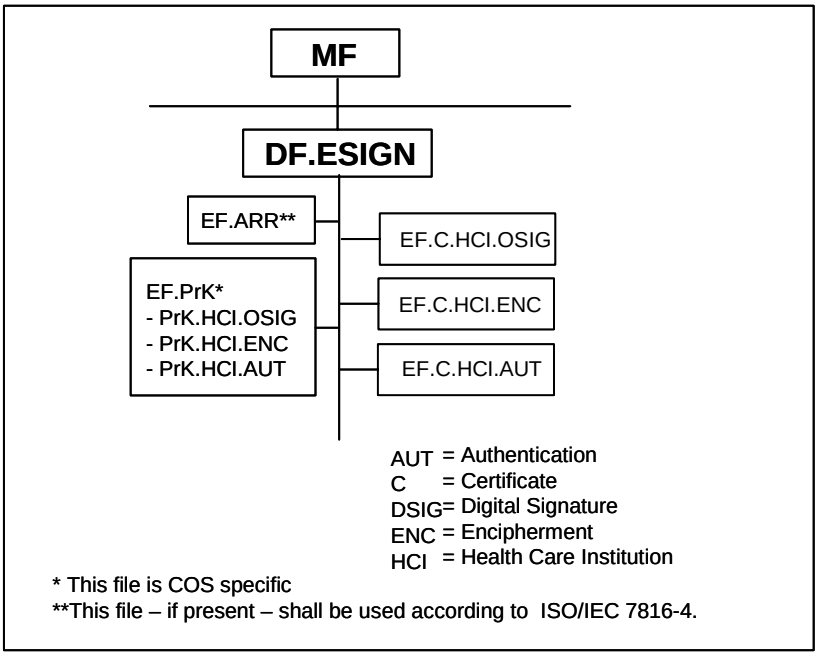

Figure 6 – General structure of DF.ESIGN

DF.ESIGN is used for

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

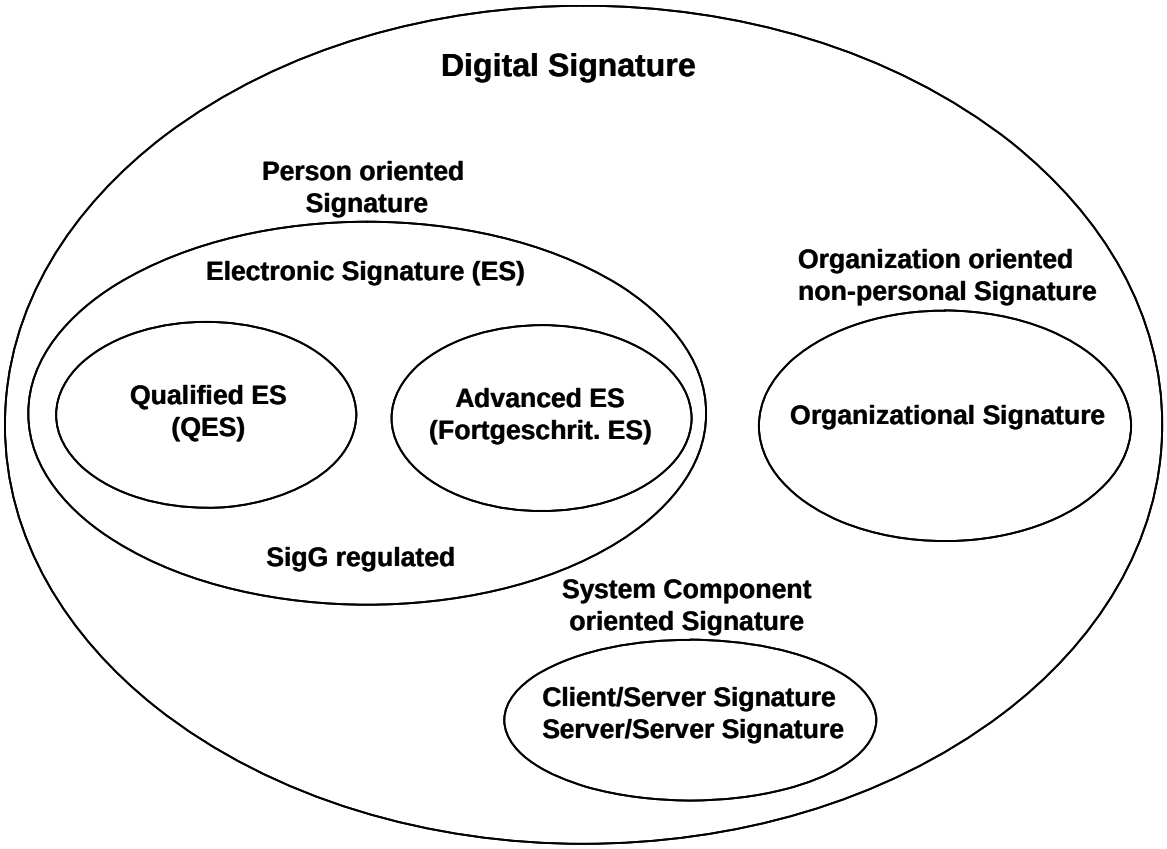

Figure 7 – Digital Signature Types

7.4.2 X.509 Certificate Files

EF.HCI.OSIG, EF.HCI.ENC and EF.C.HCI.AUT contain the X.509 certificates for the respective services. File IDs and access rules are specified in Annex B.

7.4.3 EF.PrK

EF.PrK contains the private keys as shown in the subsequent table.

Table 41 - Private key characteristics

Key Name	Key ID	Key Length see note	Access Condition
PrK.HCI.DSIG	'84'	1792 bit RSA	PIN.SMC
PrK.HCI.ENC	'83'	1792 bit RSA	PIN.SMC
PrK.HCI.AUT	'82'	1792 bit RSA	PIN.SMC

The key length should be chosen less or equal to the key length for qualified electronic signatures, whereby the minimum length has still to be compliant with the security requirements according to the protection profile [PP-SMC].

7.4.4 Reading X.509 Certificates

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

7.4.5 Key usage

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 DS command, the same command sequence as described in [HPC-P2], Clasue 8.6 is applied.

The deciphering of a document encipher key with the PSO: DECIPHER command is specified in [HPC-P2], Clause 9.7.

The client-server authentication is performed as decribed in [HPC-P2], Clause 9.6.

Annex A
(normative)

File Attributes and Access Rules

A.1 Access Rules

If a COS does not support EF.ARR, the functionality has to be ensured by other means. SMCs with EF.ARR may allow read access to the stored access rules. Therefore the security condition for the READ RECORD command related to EF.ARR is set to "always".

The specified access rules represent coding examples. They may be supported as such or by other codings, but he same functionality has to be achieved.

The MANAGE CHANNEL command is implicit allowed always and has to be send in plaintext mode.

A.2 SMC Type A, MF Level

At MF level, SE # 1 and SE # 2 are used. The access rules are SE independent, if not specified otherwise.

Table A.1 – EFs at MF level and their characteristics

File	**FID / SFID**	**File structure**	**File size** (length of data)	**Access condition**
EF.ARR (Access Rules)	COS specific	linear variable	6, 9 or 10 records with x byte, see note	ARR # 1
EF.ATR (ATR Extension Data)	'2F01' / 29	transparent	32 byte	ARR # 1
EF.DIR (Application Directory)	'2F00' / 30	linear variable	1 record with 10 byte	ARR # 1
EF.GDO (Global Data Objects)	'2F02' / 2	transparent	12 byte	ARR # 1
EF.CVC.SMC.AUT (Card Verifiable Certificate)	'2F03' / 3	transparent	209 byte	ARR # 1
EF.CVC.CA_SMC.CS (Card Verifiable Certificate)	'2F04' / 4	transparent	210 byte	ARR # 1

NOTE – The number of records depend on the TC support method:
- 6 records for SMCs with TC support method = ENVELOPE
- 9 records for SMCs with TC support method = PSO
- 10 records for SMCs with TC support method = ENVELOPE and PSO.

Table A.2 – Access Rules in EF.ARR at MF level

Rec-No.	**Value**	**Meaning**
1	'80 01 01 9000'	AM: READ RECORD / READ BINARY SC: Always Referenced in EF.ARR, EF.GDO , EF.ATR, EF.DIR, EF.CVC.CA_SMC.CS and EF.CVC.SMC.AUT
2	'87 03 2A00AE 9000'	AM: VERIFY CERTIFICATE SC: Always Referenced in EF.PuK by PuK.RCA.CS

3 (SMC with profile ID 1 (eKiosk) and 2 (hospital))	'84 01 88' 'A0 3C A4 0D 950180 5F4C 07 D276000040002A A4 0D 950180 5F4C 07 D276000040003A A4 0D 950180 5F4C 07 D276000040004A A4 0D 950180 5F4C 07 D276000040005A'	AM: INTERNAL AUTHENTICATE SC: OR template) {AT(UQ = ext. authentication, CHA = CHA.i with profile ID of a HP, i = 2-5), see related rows in Table A.3)} Referenced in EF.PrK by PrK.SMC.AUT, SE # 1 (related to SMC/eGK authentication without TC)
3 (SMC with profile ID 2 (physician/ dentist practice), 3 – 5)	'84 01 88' 'A4 0D 950180 5F4C 07 D27600004000xA', x = 2 or 3 or 4 or 5	AM: INTERNAL AUTHENTICATE SC: AT (UQ = external authentication, CHA = CHA of related HPC, see Table A.3) Referenced in EF.PrK by PrK.SMC.AUT, SE # 1 (related to SMC/eGK authentication without TC)
4 (SMC with profile ID 2 (hospital))	'840188' 'A0 3C A4 0D 950180 5F4C 07 D276000040002A A4 0D 950180 5F4C 07 D276000040003A A4 0D 950180 5F4C 07 D276000040004A A4 0D 950180 5F4C 07 D276000040005A'	AM: INTERNAL AUTHENTICATE SC: OR template {AT(UQ = ext. authentication, CHA = CHA.i with profile ID of a HP, i = 2-5), see related rows in Table A.3)} Referenced in EF.PrK by PrK.SMC.AUT, SE # 2 (related to SMC/eGK or SMC/HPC authentication with TC)
4 (SMC with profile ID 3-5)	'840188' 'A4 0D 950180 5F4C 07 D27600004000xA', x = 3 or 4 or 5	AM: INTERNAL AUTHENTICATE SC: AT (UQ = external authentication, CHA = CHA of related HPC, see Table A.3) Referenced in EF.PrK by PrK.SMC.AUT, SE # 2 (related to SMC/eGK or SMC/HPC authentication with TC)
4 (SMC with profile ID 6)	'840188' 'A4 0D 950180 5F4C 07 D276000040003A'	AM: INTERNAL AUTHENTICATE SC: AT (UQ = external authentication, CHA = CHA of related HPC, see Table A.3) Referenced in EF.PrK by PrK.SMC.AUT, SE # 2 (related to SMC/eGK or SMC/HPC authentication with TC)
5	'840182 9000'	AM: EXTERNAL AUTHENTICATE SC: Always

6	'84 01 C2 9000'	AM: ENVELOPE SC: Aways SE # 2 (relevant for TC support method = ENVELOPE)
7	'87032A8E80 9000'	AM: PSO: COMPUTE CC SC: Aways Referenced by SMK.HPC.MAC, SE # 2 (relevant for TC support method = PSO)
8	'87032A00A2 9000'	AM: PSO: VERIFY CC SC: Aways Referenced by SMK.HPC.MAC, SE # 2 (relevant for TC support method = PSO)
9	'87032A8680 9000'	AM: PSO: ENCIPHER SC: Aways Referenced by SMK.HPC.ENC, SE # 2 (relevant for TC support method = PSO)
10	'87032A8086 9000'	AM: PSO: DECIPHER SC: Aways Referenced by SMK.HPC.ENC, SE # 2 (relevant for TC support method = PSO)

Table A.3 – CHAs in SMC and HPC

CHA of CVC in SMC	SMC for	CHA in CVC of HPC relevant for authorization
‘D27600004000’ || ‘1A’	Profile 1 (eKiosk)	‘D27600004000’ || '2A' or '3A' or '4A' or '5A'
‘D27600004000’ || ‘2A’	Profile 2 (hospital)	‘D27600004000’ || '2A' or '3A' or '4A' or '5A'
‘D27600004000’ || ‘2A’	Profile 2 (physician/dentist practice)	‘D27600004000’ || '2A' (physician, dentist, …)
‘D27600004000’ || ‘3A’	Profile 3 (pharmacy, ...)	‘D27600004000’ || ‘3A’ (pharmacist)
‘D27600004000’ || ‘4A’	Profile 4 (...)	‘D27600004000’ || ‘4A’ (...)
‘D27600004000’ || ‘5A’	Profile 5 (...)	‘D27600004000’ || ‘5A’ (…)
‘D27600004000’ || ‘6A’	Profile 6 (Internet pharmacy)	‘D27600004000’ || '3A' (pharmacist, ...)

NOTE – The SMC in a hospital has the same access right to an eGK as a SMC in a physician practice, but the SMC in a physician practice can only be authorized by a physician’s HPC whereas a SMC in a hospital can be authorized by several health professionals as specified.

A.3 SMC Type A, DF.SMA

In DF.SMA, only SE # 1 (default SE) is used.

Table A.4 – EFs in DF.SMA and their characteristics

File	FID / SFID	File structure	File size (length of data)	Access condition
EF.ARR (Access Rules)	COS specific	linear variable	2 records with x byte	ARR # 1
EF.SMD (SMC related Data)	'D001' / 1	transparent	1 KB	ARR # 2

Table A.5 – Access Rules in EF.ARR in DF.SMA

Rec-No.	Value	Meaning
1	'80 01 01 9000'	AM: READ RECORD SC: Always Referenced in EF.ARR
2 (SMC-Profile 1 (eKiosk) or 2 (hospital))	'80 01 01 9000 '80 01 02 A0 3C A4 0D 950180 5F4C 07 D276000040002A A4 0D 950180 5F4C 07 D276000040003A A4 0D 950180 5F4C 07 D276000040004A A4 0D 950180 5F4C 07 D276000040005A'	AM: READ BINARY SC: Always AM: UPDATE BINARY SC: OR Template {AT (UQ = Ext. authentication, CHA = CHA.i of HPC, i = 2, 3, 4, 5)} Referenced in EF.SMD
2 (SMC-Profile 2 – 5)	'80 01 01 9000 '80 01 02 A4 0D 950180 5F4C 07 D27600000400xA', x = 2 or 3 or 4 or 5	AM: READ BINARY SC: Always AM: UPDATE BINARY SC: AT (UQ = Ext. authentication, CHA = CHA.i of HPC with i = 2 or 3 or 4 or 5) Referenced in EF.SMD
2 (SMC-Profile 6)	'80 01 01 9000 '80 01 02 A4 0D 950180 5F4C 07 D276000004003A'	AM: READ BINARY SC: Always AM: UPDATE BINARY SC: AT (UQ = Ext. authentication, CHA = CHA.i of HPC, i = 3) Referenced in EF.SMD

A.4 SMC Type B, MF Level

Table A.6 – EFs at MF level and their characteristics

File	**FID / SFID**	**File structure**	**File size** (length of data)	**Access condition**
EF.ARR (Access Rules)	COS specific	linear variable	7, 10 or 11 records with x byte, see note below Table A.1 and Table A.7	ARR # 1
EF.ATR (ATR Extension Data)	‘2F01’ / 29	transparent	32 byte or precise length	ARR # 1
EF.DIR (Application Directory)	‘2F00’ / 30	linear variable	2 records with x byte	ARR # 1
EF.GDO (Global Data Objects)	‘2F02’ / 2	transparent	12 byte	ARR # 1
EF.CVC.SMC.AUT (Card Verifiable Certificate)	‘2F03’ / 3	transparent	209 byte	ARR # 1
EF.CVC.CA_SMC.CS (Card Verifiable Certificate)	‘2F04’ / 4	transparent	210 byte	ARR # 1

Table A.7 – Access Rules in EF.ARR at MF level

Rec-No.	**Value**	**Meaning**
1-10	see Table A.2	
11	'86 08 2000 2400 2C00 2C01 9000'	AM: VERIFY, CHANGE RD (Option '00'), RESET RC (Options '00' and '01') SC: Always Referenced in EF.PIN by PIN.SMC

A.5 SMC Type B, DF.SMA

In DF.SMA, only SE # 1 (default SE) is used.

Table A.8 – EFs in DF.SMA and their characteristics

File	**FID / SFID**	**File structure**	**File size** (length of data)	**Access condition**
EF.ARR (Access Rules)	COS specific	linear variable	2 records with x byte	ARR # 1
EF.SMD (SMC related Data)	'D001' / 1	transparent	1 KB	ARR # 2
EF.NET (Network Configuration Data)	'D002' / 2	transparent	2 KB	ARR # 2

Table A.9 – Access Rules in EF.ARR in DF.SMA

Rec-No.	Value	Meaning
1	'80 01 01 9000'	AM: READ RECORD SC: Always Referenced in EF.ARR
2	'80 01 01 9000 '80 01 02 A4 06 950108 830101'	AM: READ BINARY SC: Always AM: UPDATE BINARY SC: AT (UQ = Knowledge based user authentication, KeyRef = PIN.SMC) Referenced in EF.SMD and EF.NET

A.6 SMC Type B, DF.ESIGN

In DF.ESIGN, only SE # 1 is used.

Table A.12 – EFs in DF.ESIGN and their characteristics

File	FID / SFID	File structure	File size (length of data)	Access condition
EF.ARR (Access Rules)	COS specific	linear variable	5 records with x byte	ARR # 1
EF.C.HCI.OSIG (Organizational Signature Certificate)	'C000' / 16	transparent	1.5 k byte or length of certificate	ARR # 1
EF.C.HCI.AUT (Authentication Certificate)	'C500' / 1	transparent	1.5 k byte or length of certificate	ARR # 1
EF.C.HCI.ENC (Encipherment Certificate)	'C200' / 2	transparent	1.5 k byte or length of certificate	ARR # 1

Table A.13 – Access Rules in EF.ARR in DF.ESIGN

Rec-Nr.	Wert	Bedeutung
1	'80 01 01 9000'	AM: READ BINARY / READ RECORD SC: Always Referenced in EF.ARR, EF.HCI.OSIG, EF.C.HCI.AUT and EF.C.HCI.ENC
2	'87 03 2A90A0 9000'	PSO: HASH SC: Always
3	'87 03 2A9E9A A406 950108 830101'	PSO: COMPUTE DS SC: AT (UQ = Knowledge based user authentication, KeyRef = PIN.SMC) Referenced in EF.PrK by PrK.HCI.OSIG
4	'840188 A4 06 950108 830101'	AM: INT. AUTHENTICATE SC: AT (UQ = Knowledge based user authentication, KeyRef = PIN.SMC) Referenced by PrK.HCI.AUT in EF.PrK
5	'87 03 2A8086 A4 06 950108 830101'	AM: PSO: DECIPHER SC: AT (UQ = Knowledge based user authentication, KeyRef = PIN.SMC) Referenced by PrK.HCI.ENC in EF.PrK

NOTE – The access rules for PIN.SMC are specified at MF level.

Annex B
(normative)

Content of EFs for Personalization

B.1 EF.ATR

Table B.1 – 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 [HPC-P1]
'66'	'xx'	'46 xx …' see Table B.2 || '47 04 86 01 D4 xx', xx see Table B.3.	DO Card Data (DO Pre-issuing data || DO Card capabilities with 4th byte = TC support method)

NOTE – In the 3rd capabilitiy byte the number of supported logical channels is set to 4. If the SMC supports more than 4 channels, then the respective value has to be set, see [7816-4], Clause 8.1.1.2.

Table B.2 – Value of DO Pre-issuing Data (Tag '46')

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

Table B.3 – Value of the 4th card capablities 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	0	ENVELOPE
						1	1	PSO and ENVELOPE

B.2 EF.DIR

Table B.4 – Application Templates in EF.DIR

Tag	L	Application Template	Meaning	Relevant for
'61'	'08'	'4F 06 D276 00004003'	Application Template with AID.SMA	SMC Type A + B
'61'	'0C'	'4F 0A A000000167 455349474E'	Application Template with AID.ESIGN	SMC Type B

B3. EF.GDO

Table B.5 – DO ICCSN in EF.GDO

Tag	L	Value	Meaning
’5A’	‘0A’	‘80276 …'	DO ICCSN

B.4 EF.CVC.CA-HP.CS and EF.CVC.SMC.AUT

In the CVC related EFs the respective CVC has to be stored (general coding: see [HPC-P1]).

B.5 EF.C.HCI.OSIG, EF.C.HCI.AUT and EF.C.HCI.ENC

In the X.509 certificate related EFs the respective certificate has to be stored.

B.6 EF.NET

In EF.NET, organizational entity specific net configuration data have to be stored, especially

- 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.