

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                              |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
|               | <p align="center"><b>Chipkarten mit Digitaler Signatur-Anwendung/<br/>Funktion nach SigG und SigV</b></p> <p align="center">Teil 4: Grundlegende Sicherheitsdienste</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | <p align="center">Vornorm</p> <p align="center"><b><u>DIN</u> V</b></p> <p align="center"><b>66291-4</b></p> |
| ICS 35.240.15 | <div data-bbox="596 304 1061 403" data-label="Section-Header"> <h2 align="center">Vornorm</h2> </div> <p>Chip cards with digital signature application/function according to SigG and SigV — Part 4: Basic security services</p> <p>Cartes à circuit intégré avec application/fonction signature digitale selon SigG et SigV — Partie 4: Services fondamentaux de sécurité</p> <p>Eine Vornorm ist das Ergebnis einer Normungsarbeit, das wegen bestimmter Vorbehalte zum Inhalt oder wegen des gegenüber einer Norm abweichenden Aufstellungsverfahrens vom DIN noch nicht als Norm herausgegeben wird.</p> <p>Zur vorliegenden Vornorm wurde kein Entwurf veröffentlicht.</p> <p>Erfahrungen mit dieser Vornorm sind erbeten an Normenausschuss Informationstechnik (NI) im DIN Deutsches Institut für Normung e. V.</p> <h3>Vorwort</h3> <p>DIN V 66291-4 wurde vom Arbeitsausschuss Identifikationskarten im Normenausschuss Informationstechnik (NI) erarbeitet. Sie beschreibt die Schnittstelle zu einer Chipkarte, die neben der elektronischen Signaturfunktion weitere Sicherheitsfunktionen wie z. B. Dokumententschlüsselung und Client-Server-Authentisierung bietet.</p> <p>DIN V 66291-4 ist als Ergänzung und Erweiterung zu DIN V 66291-1 zu sehen, in welcher die Signaturfunktion ausführlicher dargestellt ist.</p> <p>In einer Revisionsphase ist vorgesehen, DIN V 66291-1 und DIN V 66291-4 zusammenzuführen und neue Entwicklungen mit einzubeziehen.</p> <p>DIN V 66291-2 und DIN V 66291-3, in denen Personalisierungs-Modelle und Kommandos zur Personalisierung, insbesondere das Kommando zur karteninternen Schlüsselgenerierung beschrieben werden, befinden sich noch in Ausarbeitung. DIN V 66291-2 und DIN V 66291-3 sind zum Verständnis von DIN V 66291-1 und DIN V 66291-4 nicht erforderlich.</p> <p>DIN V 66291-4 wurde in Englisch verfasst, um so die Vornorm bei Normungsaktivitäten auf europäischer und internationaler Ebene nutzen zu können und sie auch für nicht-deutschsprachige Experten verwendbar zu machen.</p> <p align="right">Fortsetzung Seite 2 bis 103</p> <p align="center">Normenausschuss Informationstechnik (NI) im DIN Deutsches Institut für Normung e. V.</p> |                                                                                                              |

## Contents

|                |                                                                                           |            |
|----------------|-------------------------------------------------------------------------------------------|------------|
| <b>1</b>       | <b>Scope.....</b>                                                                         | <b>3</b>   |
| <b>2</b>       | <b>Normative references .....</b>                                                         | <b>3</b>   |
| <b>3</b>       | <b>Abbreviations and Notations .....</b>                                                  | <b>5</b>   |
| <b>3.1</b>     | <b>Abbreviations .....</b>                                                                | <b>5</b>   |
| <b>3.2</b>     | <b>Notations.....</b>                                                                     | <b>8</b>   |
| <b>4</b>       | <b>File Structure .....</b>                                                               | <b>10</b>  |
| <b>5</b>       | <b>Global Keys, Global Data and Card Verifiable Certificates.....</b>                     | <b>11</b>  |
| <b>5.1</b>     | <b>Scope.....</b>                                                                         | <b>11</b>  |
| <b>5.2</b>     | <b>Files on MF Level .....</b>                                                            | <b>11</b>  |
| <b>5.3</b>     | <b>CV Certificates.....</b>                                                               | <b>13</b>  |
| <b>5.4</b>     | <b>Reading the Global Data Objects and CV Certificates .....</b>                          | <b>13</b>  |
| <b>6</b>       | <b>Basic Security Services .....</b>                                                      | <b>14</b>  |
| <b>6.1</b>     | <b>Scope.....</b>                                                                         | <b>14</b>  |
| <b>6.2</b>     | <b>Certification Authorities and Certificates .....</b>                                   | <b>15</b>  |
| <b>6.3</b>     | <b>File structure .....</b>                                                               | <b>16</b>  |
| <b>6.4</b>     | <b>Application Selection.....</b>                                                         | <b>17</b>  |
| <b>6.5</b>     | <b>Reading of EF.SSD.....</b>                                                             | <b>18</b>  |
| <b>6.6</b>     | <b>Authentication of the Cardholder.....</b>                                              | <b>19</b>  |
| <b>6.7</b>     | <b>Digital Signature Service.....</b>                                                     | <b>20</b>  |
| <b>6.8</b>     | <b>Authentication with CV Certificates .....</b>                                          | <b>27</b>  |
| <b>6.9</b>     | <b>Client/Server Authentication.....</b>                                                  | <b>32</b>  |
| <b>6.10</b>    | <b>Encryption Key Decipherment.....</b>                                                   | <b>33</b>  |
| <b>6.11</b>    | <b>Reading X.509 Certificates and the Public Key of CAs.....</b>                          | <b>37</b>  |
| <b>6.12</b>    | <b>Change of Reference Data .....</b>                                                     | <b>38</b>  |
| <b>6.13</b>    | <b>Reset of RC and Setting a new PIN or Password .....</b>                                | <b>39</b>  |
| <b>7</b>       | <b>Cryptographic Token Information .....</b>                                              | <b>40</b>  |
| <b>7.1</b>     | <b>Scope.....</b>                                                                         | <b>40</b>  |
| <b>7.2</b>     | <b>File Structure .....</b>                                                               | <b>40</b>  |
| <b>7.3</b>     | <b>Application Selection.....</b>                                                         | <b>41</b>  |
| <b>7.4</b>     | <b>Reading Cryptographic Token Information.....</b>                                       | <b>41</b>  |
| <b>Annex A</b> | <b>(normative) Digital Signature Formats, AlgIDs and OIDs .....</b>                       | <b>43</b>  |
| <b>Annex B</b> | <b>(normative) Authentication Certificates .....</b>                                      | <b>48</b>  |
| <b>Annex C</b> | <b>(normative) File Parameter .....</b>                                                   | <b>57</b>  |
| <b>Annex D</b> | <b>(normative) Device Authentication, Session Key Agreement and Secure Messaging.....</b> | <b>62</b>  |
| <b>Annex E</b> | <b>(normative) Security Service Descriptor Templates .....</b>                            | <b>73</b>  |
| <b>Annex F</b> | <b>(informative) ATR-Coding.....</b>                                                      | <b>78</b>  |
| <b>Annex G</b> | <b>(informative) Content of Cryptographic Token Information Files.....</b>                | <b>81</b>  |
| <b>Annex H</b> | <b>(informative) Identification Data .....</b>                                            | <b>98</b>  |
| <b>Annex I</b> | <b>(informative) Improvements of DIN V 66291-4 versus DIN V 66291-1 .....</b>             | <b>102</b> |
|                | <b>Bibliography .....</b>                                                                 | <b>103</b> |

## Foreword

This specification is in full compliance with the Office Identity Card (OIC) specified by TeleTrust Deutschland e.V.

## 1 Scope

This specification defines the interface between a terminal (interface device) and a card with “Basic Security Services”. It

- is compliant with the Office Identity Card (OIC) specification
- covers DIN V 66291-1 and
- is in compliance with the German digital signature law and the EU directive for electronic signatures.

The following basic security services are specified:

- digital signature service
- authentication service for logon, client/server authentication and ICC/IFD authentication
- encryption service for document encryption.

All defined codings for commands and data are based on ISO/IEC 7816, parts 4, 5, 6, 8 and 9. Applications with other codings shall comply with the functional requirements. For the transmission level, the specifications in DIN V 66291-1 apply.

## 2 Normative references

This Prestandard incorporates by dated or undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this Prestandard only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

DIN V 66291-1:1999, *Chipkarten mit digitaler Signatur-Anwendung/Funktion nach SigG/SigV — Teil 1: Anwendungsschnittstelle*

ISO 9564-1:1991, *Banking; Personal identification number management and security — Part 1: PIN protection principles and techniques*

ISO/IEC 7816-3:1997, *Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 3: Electronic signals and transmission protocols*

ISO/IEC 7816-4:1995, *Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 4: Interindustry commands for interchange, AM1: Impact of secure messaging on the structures of APDU messages*

ISO/IEC 7816-4 AMD1:1997, *Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 4: Interindustry commands for interchange, Amendment 1: Impact of secure messaging on the structures of APDU messages*

ISO/IEC 7816-5:1994, *Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 5: Numbering system and registration procedure for application identifiers*

ISO/IEC 7816-6:1996, *Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 6: Interindustry data elements*

ISO/IEC 7816-8:1999, *Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 8: Security related interindustry commands*

ISO/IEC 7816-9:2000, *Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 9: Additional interindustry commands and security attributes*

ISO/IEC CD 7816-15.2:2001, *Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 15: Cryptographic Token Application*

ISO/IEC 8825:1990, *Information technology — Open systems interconnection — Specification of basic encoding rules for abstract syntax notation one (ASN.1)*

ISO/IEC 9796-2:1997, *Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Mechanisms using a hash-function*

ISO/IEC 9797-1:1999, *Information technology — Security techniques — Message authentication codes, Part 1: Mechanisms using a block cipher*

ISO/IEC 9798-3:1993, *Information technology — Security techniques — Entity authentication mechanisms — Part 3: Entity authentication using a public key algorithm*

ISO/IEC 9798-3:1998, *Information technology — Security techniques — Entity authentication — Part 3: Mechanisms using digital signature techniques*

ISO/IEC 11770-3:1999, *Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques*

ANSI X 9.19:1996, *Financial Institution Retail Message Authentication*

ANSI X 9.62, Draft, *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm*, 1999

ANSI X 9.63 Working Draft, Version 2.0, *Public Key Cryptography for the Financial Services Industry: Elliptic Curve Key Agreement and Key Transport Schemes*, 5. July 1998

Curve Key Agreement and Key Transport Schemes, 1999

German digital signature law — Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz — SigG), 21. Mai 2001

German signature ordinance — Verordnung zur elektronischen Signatur (Signaturverordnung — SigV), August 2001 (not yet finalized)

IEEE P1363, Standard Specifications for Public Key Cryptography, 2000

NIST: FIPS Publication 180-1: Secure Hash Standard (SHS-1), Mai 1995

NIST: FIPS Publication 186-2: Digital Signature Standard (DSS), 2000

PKCS #1: RSA Encryption Standard, Version 1.5, Nov. 1993

PKCS #1: RSA Encryption Standard, Version 2.0, July 1998

PKCS #15: Cryptographic Token Information Format Standard, 3rd Draft Version 1.1, May 4, 2000 (see also ISO/IEC 7816-15, which supersedes PKCS #15)

RFC 1510: The Kerberos Network Authentication Service (V5), September 1993

RFC 2631: Diffie-Hellman Key Agreement Method, June 1999

RFC 2785: Methods for Avoiding the “Small-Subgroup” Attacks on the Diffie-Hellman Key Agreement Method for S/MIME, March 2000

### 3 Abbreviations and Notations

#### 3.1 Abbreviations

|     |   |                                  |
|-----|---|----------------------------------|
| AID | = | Application Identifier           |
| ASS | = | Additional Security Services     |
| AKI | = | Authority Key Identifier         |
| ATR | = | Answer-to-Reset                  |
| AUT | = | Authentication                   |
| B   | = | Byte                             |
| BCD | = | Binary Coded Digit               |
| BD  | = | Basic Identification Data        |
| BER | = | Basic Encoding Rules             |
| BSS | = | Basic Security Services          |
| C   | = | Certificate                      |
| CA  | = | Certification Authority          |
| CAR | = | CA Reference                     |
| CC  | = | Cryptographic Checksum           |
| CG  | = | Cryptogram                       |
| CH  | = | Cardholder                       |
| CHA | = | Certificate Holder Authorisation |
| CHN | = | Cardholder Name                  |
| CHR | = | Certificate Holder Reference     |
| CRT | = | Control Reference Template       |
| CPI | = | Certificate Profile Identifier   |
| CS  | = | CertSign                         |

|       |   |                                 |
|-------|---|---------------------------------|
| CT    | = | CRT for confidentiality         |
| CTI   | = | Cryptographic Token Information |
| CV    | = | Card Verifiable                 |
| C/S   | = | Client/Server                   |
| D()   | = | Decipherment of                 |
| DE    | = | Data Element                    |
| DF    | = | Dedicated File                  |
| DH    | = | Diffie-Hellman                  |
| DO    | = | Data Object                     |
| DS    | = | Digital Signature               |
| DSA   | = | Digital Signature Algorithm     |
| DSI   | = | Digital Signature Input         |
| DST   | = | CRT for Digital Signature       |
| E()   | = | Encipherment of                 |
| ED    | = | Enhanced Identification Data    |
| EF    | = | Elementary File                 |
| ELC   | = | Elliptic Curve                  |
| FCI   | = | File Control Information        |
| FID   | = | File Identifier                 |
| GDO   | = | Global Data Objects             |
| h()   | = | hash value of                   |
| HB    | = | Historical Bytes                |
| HT    | = | CRT for hash code               |
| ICC   | = | Integrated Circuit(s) Card      |
| ICCSN | = | ICC Serial Number               |
| IDD   | = | Identification Data             |
| IFD   | = | Interface Device                |
| IFSC  | = | Information Field Size Card     |
| IFSD  | = | Information Field Size Device   |
| IVS   | = | Identity Verification System    |

|       |   |                                                |
|-------|---|------------------------------------------------|
| KE    | = | Key Encipherment                               |
| KID   | = | Key Identifier                                 |
| MF    | = | Master File                                    |
| MSE   | = | MANAGE SEC. ENVIRONMENT                        |
| NAD   | = | Node Address                                   |
| OIC   | = | Office Identity Card                           |
| OID   | = | Object Identifier                              |
| PCA   | = | Policy Certification Authority                 |
| PK    | = | Public Key                                     |
| PKCS  | = | Public Key Cryptography Standards              |
| PI    | = | Padding Indicator                              |
| PIN   | = | Personal Identification Number                 |
| PRND  | = | Padding Random Number                          |
| PROV  | = | Provider                                       |
| PPS   | = | Protocol Parameter Selection                   |
| PSO   | = | PERFORM SEC. OPERATION                         |
| PV    | = | Plain Value                                    |
| PW    | = | Password                                       |
| RC    | = | Retry Counter                                  |
| RCA   | = | RootCA                                         |
| RD    | = | Reference Data                                 |
| RegTP | = | Regulation Authority Telecom & Post            |
| RFU   | = | Reserved for Future Use                        |
| RSA   | = | Signature Algorithm of Rivest, Shamir, Adleman |
| SE    | = | Security Environment                           |
| SIG() | = | Signature of                                   |
| SigG  | = | Signature law                                  |
| SK    | = | Secret Key                                     |
| SN    | = | Serial Number                                  |
| SM    | = | Secure Messaging                               |

|      |   |                                                    |
|------|---|----------------------------------------------------|
| SP   | = | Specific Privileges                                |
| SSC  | = | Send Sequence Counter                              |
| SSD  | = | Security Service Descriptor                        |
| TLS  | = | Transport Layer Security                           |
| TLV  | = | Tag, Length, Value                                 |
| TTT  | = | Teletrust OID Registration Authority <sup>1)</sup> |
| VD   | = | Verification Data                                  |
| VR   | = | Verification Requirement                           |
| WTLS | = | Wireless TLS                                       |
| ZZ   | = | Diffie-Hellman shared value                        |

### 3.2 Notations

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

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

<key descriptor> ::=

<key>[<index1>].<keyholder>

[<index2>].<usage list>

<key> ::= <asymmetric key> | <symmetric key>

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

<secret key> ::= SK

<public key> ::= PK

<index1> ::= 1 | 2 | ...

<keyholder> ::= <cardholder> | <device> | <organisation>

<device> ::= <integrated circuit(s) card> | <interface device> | <personalisation system> | <server> |

<identity verification system>

<organisation> ::= <certification authority> | <card manufacturer>

<cardholder> ::= CH

<certification authority> ::= CA | RCA

<card manufacturer> ::= CM

---

1) see [www.teletrust.de](http://www.teletrust.de)

<integrated circuit(s) card>::= ICC  
 <interface device>::= IFD  
 <personalisation system>::= PS  
 <server> ::= S  
 <identity verification system> ::= IVS  
 <index2> used for indication of qualification or role  
 <usage list>::= <usage>[<index3>] | <usage list> & <usage>[<index3>]  
 <usage>::= <digital signature> | <authentication> | <key encipherment> |<CertSign>  
 <digital signature>::= DS  
 <authentication>::= AUT  
 <key encipherment>::= KE  
 <CertSign> ::= CS | CS-DS | CS-AUT | CS-KE  
 <index3> used for indication of algorithm or components (e.g. ICC/IFD or C/S)  
 <certificate descriptor>::= <certificate>[<index1>].  
 <certholder>[<index2>].  
 <usage list>  
 <certificate>::= C | <CV certificate> | <X.509 certificate> | <X.509 attribute certificate>  
 <CV certificate> ::= C\_CV  
 <X.509 certificate> ::= C\_X509  
 <X.509 attribute certificate> ::= C\_X509A  
 <certholder>::= <cardholder> | <device> | <organisation>

NOTE      Indexes shall only be applied to avoid ambiguity.

For the representation of data sequences the following notation is used:

||      = Concatenation of data

EXAMPLE 1      SK.RCA.CS = Secret key of root CA for signing certificates, whereby no binding of the certified key pair to a special usage is specified

EXAMPLE 2      SK.RCA.CS-DS = Secret key of root CA for signing certificates, whereby the certified key pair shall be used for signing DS certificates only

EXAMPLE 3      SK<sub>1</sub>.CH.DS<sub>RSA</sub> = Secret key no. 1 of the cardholder for digital signature with RSA

EXAMPLE 4      SK.CH.AUT<sub>C/S</sub> = Secret key of the cardholder for client/server authentication

EXAMPLE 5      PK.CA.CS-AUT<sub>C/S</sub> = Public key of CA for verification of certificates related to client/server authentication

EXAMPLE 6 PK.CA.CS-AUT<sub>ICC/IFD</sub> = Public key of CA for verification of certificates related to ICC/IFD authentication

EXAMPLE 7 SK.CA.CS-AUT&AUT = Secret key of CA for signing of authentication certificates and for use in authentication procedures

## 4 File Structure

The card has a general file structure according to figure 1 or figure 2.

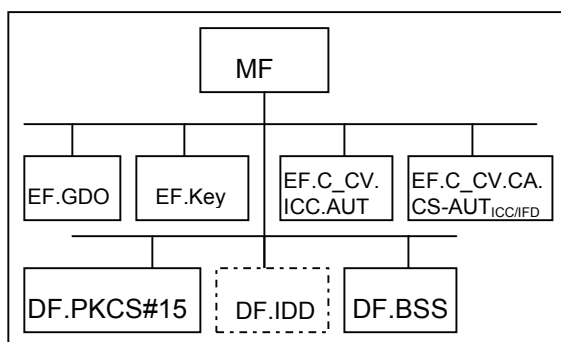


Figure 1 — File structure with DF.BSS

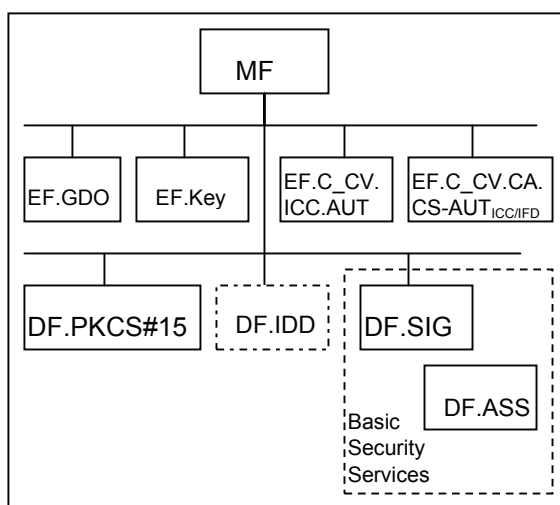


Figure 2 — File structure with DF.SIG and DF.ASS

The logical place of DF.ASS may be under DF.SIG or under MF. The functionality of DF.SIG together with DF.ASS is that of DF.BSS.

The relevant Application Identifiers are shown in table 1.

Table 1 — AIDs

| Name       | AID                        |
|------------|----------------------------|
| DF.PKCS#15 | 'A000000063504B43532D3135' |
| DF.IDD     | 'D27600006603'             |
| DF.BSS     | 'D27600006601'             |
| DF.SIG     | 'D27600006601'             |
| DF.ASS     | 'D27600006602'             |

NOTE In the new ISO/IEC 7816-15 standard on Cryptographic Token Information, the name of the related DF is DF.CTI with AID 'E800000001435449'

DFs shall have an FID, so that e.g. an absolute path to an EF can be described in the cryptographic token information.

## 5 Global Keys, Global Data and Card Verifiable Certificates

### 5.1 Scope

This clause specifies the global keys, the global data objects and CV certificates.

### 5.2 Files on MF Level

Figure 3 shows the elementary files at MF level.

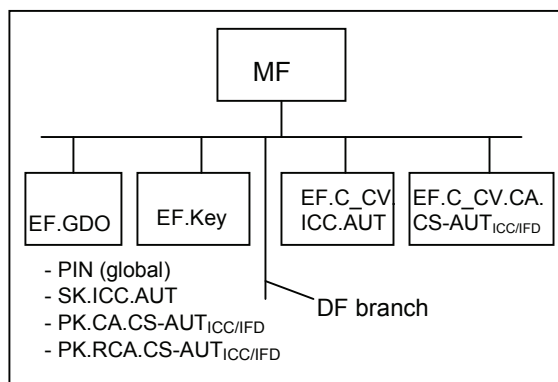


Figure 3 — EFs at MF Level

#### 5.2.1 EF.GDO

The EF.GDO contains

- DO 'ICC Serial Number (ICCSN)' as shown in figures. 4 or 5 (tag '5A', also referred to as primary account number) and
- DO 'Cardholder Name (CHN)' as shown on the card cover (tag '5F20'). The DO CHN is optional.

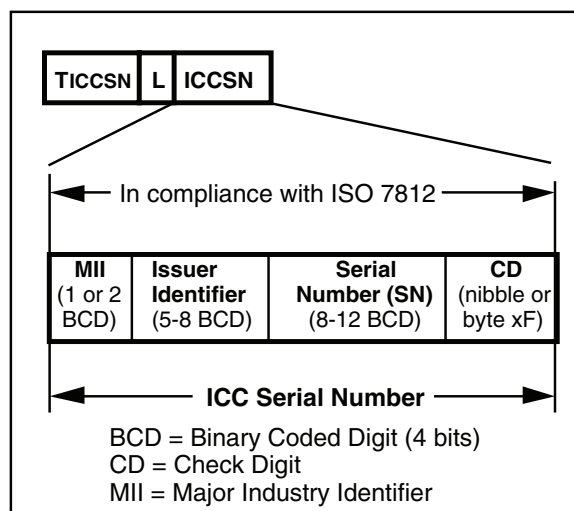


Figure 4 — ICCSN (in compliance with ISO/IEC 7812)

An alternative encoding for the ICCSN is shown in figure 5.

| Issuer Identification No. | Serial No.                      |
|---------------------------|---------------------------------|
| 'D2 76 nn nn nn'          | 'xx .. xx'                      |
| (5 Bytes, n = BCD)        | (8 Bytes, e.g. chip serial no.) |

Figure 5 — ICCSN (ISO/IEC 7816-5/6-oriented with Category D and Country Code)

NOTE An IIN according to figure 5 is assigned by CCG<sup>2)</sup> in Cologne.

### 5.2.2 EF.Key

There may be one or more key files with private keys. The private keys shown in table 2 are present:

Table 2 — Keys and KIDs

| Key name                                                                     | KID  |
|------------------------------------------------------------------------------|------|
| PIN (global, authentication and decryption PIN)                              | '01' |
| SK.ICC.AUT <sub>ICC/IFD</sub> (secret key of ICC for ICC/IFD authentication) | '01' |

NOTE If other KIDs are used, then the KID has to be indicated in the SSD file or in the cryptographic token information.

In addition to the private keys, the public key of the root CA and the CA which issued the CV certificate are present in a key file at MF level: PK.RCA.CS-AUT<sub>ICC/IFD</sub>.

PK.CA.CS-AUT<sub>ICC/IFD</sub>

### 5.2.3 EF.C\_CV.ICC.AUT

The EF.C\_CV.ICC.AUT contains the CV certificate of the card for authentication.

2) Centrale für Coorganisation GmbH, Maarweg 133, 50825 Köln

#### 5.2.4 EF.C\_CV.CA.CS-AUT<sub>ICC/IFD</sub>

The EF.C\_CV.CA.CS-AUT<sub>ICC/IFD</sub> contains the CV certificate of the CA or card manufacturer which issued the card certificate C\_CV.ICC.AUT.

### 5.3 CV Certificates

Besides the X.509v3 certificates, a CV certificate (see figure 6) is needed in a card to enable especially

- advanced personalisation concepts
- access to the protected employee data and
- digital signatures on public customer service terminals, where a higher security level is required (see DIN V 66291-1).

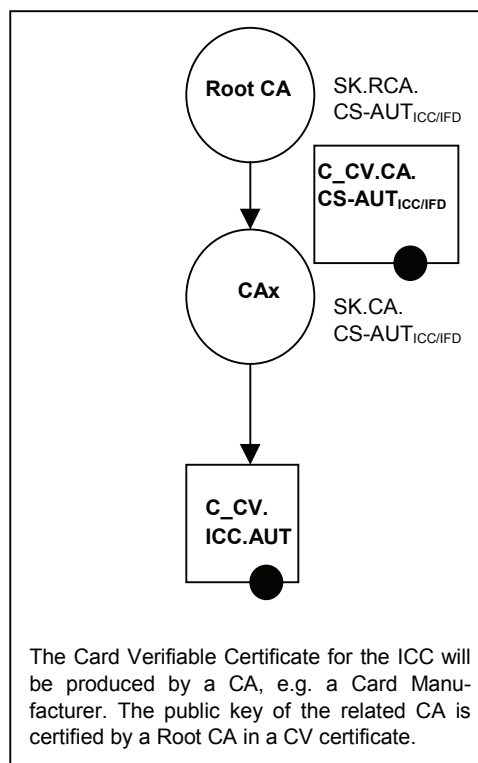


Figure 6 — CAs and CV certificates

### 5.4 Reading the Global Data Objects and CV Certificates

For reading the global data objects and CV certificates, the ISO/IEC 7816-4 commands SELECT FILE and READ BINARY are used as shown in tables 3 to 6.

**Table 3 — SELECT FILE command for EF selection**

|            |                                                                                                             |
|------------|-------------------------------------------------------------------------------------------------------------|
| CLA        | '00'                                                                                                        |
| INS        | 'A4' = SELECT FILE                                                                                          |
| P1         | '02' = EF file selection                                                                                    |
| P2         | '0C' = No FCI to return                                                                                     |
| Lc         | '02' = Length of subsequent data field                                                                      |
| Data field | FID (see annex C) of one of the files:<br>— EF.GDO<br>— EF.C.ICC.AUT<br>— EF.C.CA.CS-AUT <sub>ICC/IFD</sub> |
| Le         | Empty                                                                                                       |

**Table 4 — SELECT FILE response**

|            |                                 |
|------------|---------------------------------|
| Data field | Empty                           |
| SW1-SW2    | '9000' or specific status bytes |

**Table 5 — READ BINARY command for reading the global data objects or CV certificates**

|            |                    |
|------------|--------------------|
| CLA        | '00'               |
| INS        | 'B0' = READ BINARY |
| P1,P2      | '0000'             |
| Lc         | Empty              |
| Data field | Empty              |
| Le         | '00'               |

**Table 6 — READ BINARY response**

|            |                                                                                                                                                 |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Data field | — If EF.GDO: Global data objects<br>— If EF.C_CV.ICC.AUT: CV certif. of ICC<br>— If EF.C_CV.CA.CS-AUT <sub>ICC/IFD</sub> : CV certificate of CA |
| SW1-SW2    | '9000' or specific status bytes                                                                                                                 |

## 6 Basic Security Services

### 6.1 Scope

The basic security services provided by DF.BSS cover the

- digital signature service for legally relevant signatures of the cardholder
- authentication service as required for specific authentication procedure

— Key decipherment service

The digital signature service is in full compliance with DIN V 66291-1.

## 6.2 Certification Authorities and Certificates

The basic security mechanisms require different types of end user certificates:

- DS certificate(s) (X.509v3 digital signature certificate(s), i.e. public key certificate and attribute certificate(s)); key usage flag is set to “non-repudiation”
- AUT<sub>C/S</sub> certificate (X.509v3 authentication certificate) for proving access rights to servers; key usage flag is set to “digital signature”
- KE certificate (X.509v3 key encipherment certificate); key usage flag is set to “key encipherment or key agreement”.

NOTE 1 In principle it is also possible to set the flags for “digital signature” and “key encipherment/agreement” in the same certificate, if appropriate.

The X.509v3 certificates have to be produced by certification authorities (CA) as shown in figure 7.

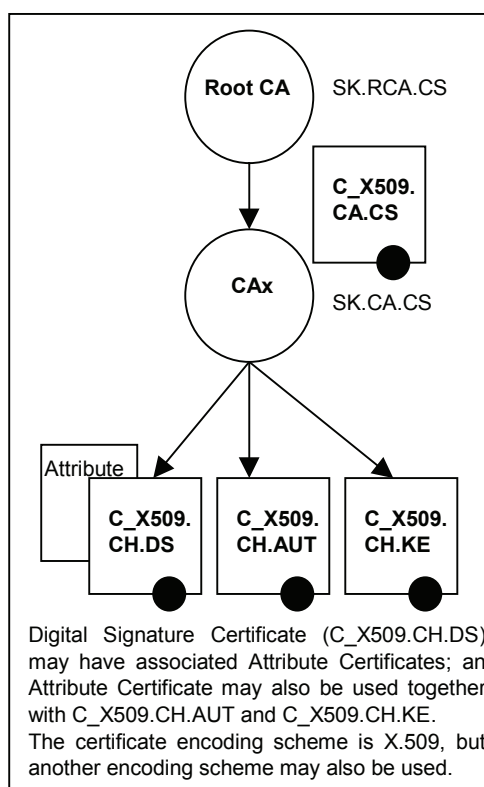


Figure 7 — CAs and X.509v3 certificates (example)

NOTE 2 The root CA for the digital signature service and for the other security services may not be the same. In case that there is a common root, it may be that different keys are used for signing DS-related certificates and certificates related to the other security services.

## 6.3 File structure

### 6.3.1 General file structure

Figure 8 shows the BSS file structure.

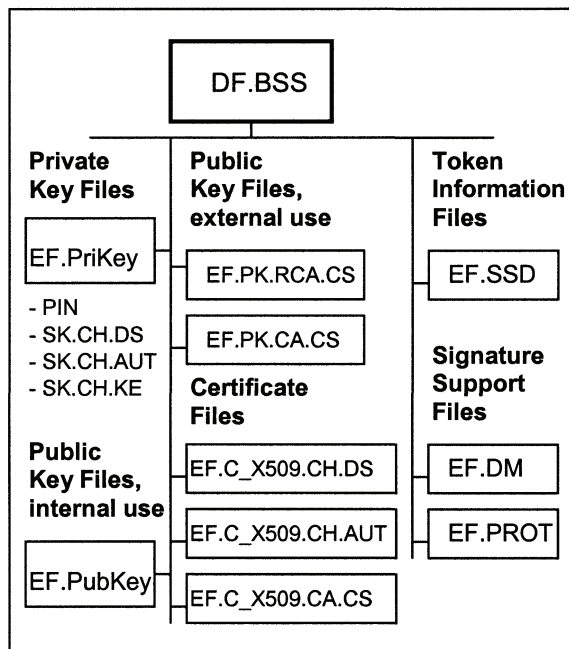


**Figure 8 — BSS file structure (example)**

**NOTE** The certificate for key enciphering is normally stored in Directory Systems and not in the card. However, depending on the client/server authentication mechanism encipherment may also play a role.

### 6.3.2 EF.PriKey

There may be one or more key files with private keys. The private keys shown in table 7 are present:

**Table 7 — Keys and KIDs**

| Key name                              | KID              |
|---------------------------------------|------------------|
| PIN (specific, digital signature PIN) | '81'             |
| SK.CH.DS (digital signature key)      | implicit or '84' |
| SK.CH.AUT (authentication key)        | '82'             |
| SK.CH.KE (key encipherment key)       | '83'             |

**NOTE** If other KIDs are used, then the KID has to be indicated in the SSD file or in the cryptographic token information.

### 6.3.3 EF.PubKey

In the optional public key file(s) for internal use, PKs are stored to be applied by the card for signature verification (e.g. the PKs of special communication partners may be installed in the personalisation phase). For the signature verification service the command VERIFY SIGNATURE has to be applied as specified in DIN V 66291-1.

#### **6.3.4 EF.PK.RCA.CS**

In public key files for external use, PKs are stored to be applied by the outside world:

— PK.RCA.CS (verification key for X509 certificates of the root CA).

#### **6.3.5 EF.PK.CA.CS**

In public key files for external use, PKs are stored to be applied by the outside world:

— PK.CA.CS (verification key for X509 certificates of the CA issuing the certificates C.CH.x).

#### **6.3.6 EF.C\_X509.CH.DS**

The EF.C\_X509.CH.DS contains the DS-certificate of the cardholder.

#### **6.3.7 EF.C\_X509.CA.CS**

The EF.C\_X509.CA.CS contains the X.509v3 certificate of the CA which issued the cardholder certificates.

#### **6.3.8 EF.C\_X509.CH.AUT**

The EF.C\_X509.CH.AUT contains the AUT-X.509v3 certificate of the cardholder.

#### **6.3.9 EF.SSD**

The EF.SSD contains the security service descriptor templates as defined in annex G (identical with DIN V 66291-1, only the DO PIN usage policy has been extended).

#### **6.3.10 EF.DM**

The EF.DM contains the display message. It should consist of 8 characters in ASCII Code and be pronounceable (have a meaning for the cardholder) so that the cardholder can recognise it easily when it is displayed.

#### **6.3.11 EF.PROT**

The optional file EF.PROT with cyclic file structure serves as a logfile for signatures. It is to be seen as an aid for the user, but cannot be used as legal evidence. A record contains:

- Date (12 Bytes, JJJJMMDDHHMM),
- Terminal ID (18 Bytes, e.g. ICCSN.IFD in printable form),
- Document-ID (20 Bytes) and
- Signature counter (3 Bytes, digits).

ASCII shall be used as the coding scheme.

### **6.4 Application Selection**

The ISO/IEC 7816-4 command for 'Direct Application Selection' is shown in the two subsequent tables 8 and 9.

**Table 8 — SELECT FILE command for application selection with AID**

|            |                                             |
|------------|---------------------------------------------|
| CLA        | '00'                                        |
| INS        | 'A4' = SELECT FILE                          |
| P1         | '04' = DF selection by AID                  |
| P2         | '0C' = No FCI to return                     |
| Lc         | '06' = Length of subsequent data field      |
| Data field | 'D27600006601' = AID of DF.BSS, see table 1 |
| Le         | Empty                                       |

**Table 9 — SELECT FILE response**

|            |                                 |
|------------|---------------------------------|
| Data field | Empty                           |
| SW1-SW2    | '9000' or specific status bytes |

## 6.5 Reading of EF.SSD

For reading the security service descriptors needed by the outside world, the commands shown in tables 10 to 13 are needed:

**Table 10 — SELECT FILE command for selecting EF.SSD**

|            |                                        |
|------------|----------------------------------------|
| CLA        | '00'                                   |
| INS        | 'A4' = SELECT FILE                     |
| P1         | '02' = EF file selection               |
| P2         | '0C' = No FCI to return                |
| Lc         | '02' = Length of subsequent data field |
| Data field | FID of EF.SSD, see annex C             |
| Le         | Empty                                  |

**Table 11 — SELECT FILE response**

|            |                                 |
|------------|---------------------------------|
| Data field | Empty                           |
| SW1-SW2    | '9000' or specific status bytes |

**Table 12 — READ BINARY command**

|            |                    |
|------------|--------------------|
| CLA        | '00'               |
| INS        | 'B0' = READ BINARY |
| P1,P2      | '0000'             |
| Lc         | Empty              |
| Data field | Empty              |
| Le         | '00'               |

**Table 13 — READ BINARY response**

|            |                                 |
|------------|---------------------------------|
| Data field | SSD templates                   |
| SW1-SW2    | '9000' or specific status bytes |

## 6.6 Authentication of the Cardholder

The DF.BSS contains a specific local PIN dedicated to protect the COMPUTE DIGITAL SIGNATURE operation.

For protection of the client/server authentication function and the key decipherment function a global PIN is used.

In a future version of this specification, biometrical user authentication may be added.

**Table 14 — VERIFY command for cardholder authentication**

|            |                                                                                                                                                    |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| CLA        | '00'                                                                                                                                               |
| INS        | '20' = VERIFY                                                                                                                                      |
| P1         | '00'                                                                                                                                               |
| P2         | '81' = Specific PIN/PW reference for DS, see table 15<br>'01' = Global PIN/PW reference for AUT+KE, see table 2                                    |
| Lc         | '0x' = Length of subsequent data field                                                                                                             |
| Data field | PIN or PW (min 6, max 8 ASCII digits or characters) or<br>PIN in Format 2 PIN Block (see ISO 9564-1), if this format is indicated in the SSD file. |
| Le         | Empty                                                                                                                                              |

NOTE The VERIFY command referencing the global PIN may be sent at any time after answer-to-reset.

**Table 15 — VERIFY response**

|            |                                 |
|------------|---------------------------------|
| Data field | Empty                           |
| SW1-SW2    | '9000' or specific status bytes |

After successful presentation of PIN or PW, the retry counter is automatically reset to its initial value (value 3).

The following Status Bytes are of special importance:

- '6300': Warning – verification failed (no further information)
- '63Cx': Warning – verification failed (x indicates the number of further allowed retries)

— '6983': Checking error: authentication method blocked (these status bytes shall be delivered if the VERIFY command is sent and the RC is zero).

## 6.7 Digital Signature Service

### 6.7.1 General Aspects

The digital signature function is in full compliance with DIN V 66291-1. A digital signature process consists of several steps as shown in figure 9.

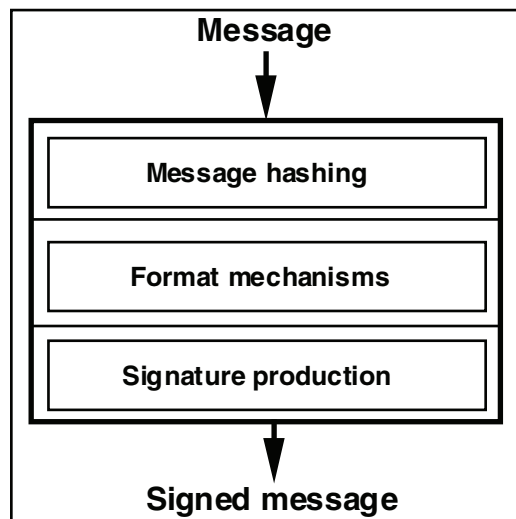


Figure 9 — Signature process

#### Step 1: Message hashing

The text to be signed has to be hashed by applying a hash function which is on the list of the applicable hash functions (see annex A).

The hash result can be considered as a compressed version of the text. The hashing will be done either

- outside the card or
- inside the card or
- partly outside and partly inside (last round of hashing) the card,

depending on the card functionality and the software organisation.

#### Step 2: Format mechanisms

Since the hash result may be shorter than the Digital Signature Input (DSI) for signature production, the hash value has to be padded, i.e. to be formatted. The padding, however, is not a simple filling up with a special padding character, since the construction of the DSI is highly security relevant. Several format mechanisms have been defined, some of them are evaluated as “weak” and should not be used.

#### Step 3: Signature production

The final DSI is the string to be transformed by the signature algorithm. The result is the Digital Signature DS.

The command sequence for signature computation depends on the functionality of the respective card (cards without and with a hash algorithm as shown in figures 10 and 11).

| ICC Commands                                                                                                                              | Meaning                                                      |
|-------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|
| <b>PSO: COMPUTE DS</b><br><hash value or digestinfo><br> | Computation of a digital signature (command can be repeated) |

Figure 10 — Digital signature phase – card without hash algorithm

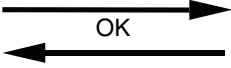
| ICC Commands                                                                                                                                   | Meaning                                                      |
|------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|
| <b>PSO: HASH</b> <Inter-mediate hash result    textblock><br> | Hashing the last round in the card                           |
| <b>PSO: COMPUTE DS</b><br>                                    | Computation of a digital signature (command can be repeated) |

Figure 11 — Digital signature phase – card with hash algorithm

## 6.7.2 Signature Computation without Hashing

The ISO/IEC 7816-8 command for digital signature computation is shown in table 16. If there is only one signature key, then this key may be implicitly selected (if not, the KID has to be set with the MSE command).

Signature algorithm and allowed Digital-Signature-Input formats (DSI formats) are outlined in annex A.

Table 16 — PSO: COMPUTE DS command

|            |                                                                                                                                                                            |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CLA        | As defined in ISO/IEC 7816-4 and -8                                                                                                                                        |
| INS        | '2A' = PERFORM SECURITY OPERATION: COMPUTE DIGITAL SIGNATURE                                                                                                               |
| P1         | '9E' = Return digital signature                                                                                                                                            |
| P2         | '9A' = Data field contains data to be integrated in the DSI                                                                                                                |
| Lc         | 'xx' = Length of subsequent data field                                                                                                                                     |
| Data field | Data to be integrated in the DSI: hash value or digestinfo, see annex A<br>(the length of the data field shall not exceed 40% of the length of the modulus in case of RSA) |
| Le         | '00' or 'xx' = Length of expected digital signature                                                                                                                        |

**Table 17 — PSO: COMPUTE DS response**

|            |                                 |
|------------|---------------------------------|
| Data field | Digital signature               |
| SW1-SW2    | '9000' or specific status bytes |

### 6.7.3 Signature Computation with Hashing

Cards with a hash function (see annex A) can compute the final hash value by processing the last round(s) in the card. The ISO/IEC 7816-8 command for hashing is PSO: HASH. See table 18.

The command can also be used for delivering the complete hash value to the card.

**Table 18 — PSO: HASH command**

|            |                                                                                                                                                                                                                                               |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CLA        | As defined in ISO/IEC 7816-4 and -8                                                                                                                                                                                                           |
| INS        | '2A' = PERFORM SECURITY OPERATION: HASH                                                                                                                                                                                                       |
| P1         | '90' = Compute hash value                                                                                                                                                                                                                     |
| P2         | 'A0' = Data field contains DOs relevant for hashing                                                                                                                                                                                           |
| Lc         | 'xx' = Length of subsequent data field                                                                                                                                                                                                        |
| Data field | <ul style="list-style-type: none"> <li>— If data shall be hashed: '90' – L – Intermediate hash result (see annex A)    '80' – L – Data to be hashed</li> <li>— If the final hash value shall be transmitted: '90' – L – Hash value</li> </ul> |
| Le         | Empty                                                                                                                                                                                                                                         |

**Table 19 — PSO: HASH response**

|            |                                 |
|------------|---------------------------------|
| Data field | Empty                           |
| SW1-SW2    | '9000' or specific status bytes |

After hashing the PSO: COMPUTE DIGITAL SIGNATURE command has to be sent. See table 20.

**Table 20 — PSO: COMPUTE DS command**

|            |                                                                       |
|------------|-----------------------------------------------------------------------|
| CLA        | As defined in ISO/IEC 7816-4 and -8                                   |
| INS        | '2A' = PERFORM SECURITY OPERATION: COMPUTE DIGITAL SIGNATURE          |
| P1         | '9E' = Return digital signature                                       |
| P2         | '9A' = Data field contains data to be signed or integrated in the DSI |
| Lc         | Empty                                                                 |
| Data field | Empty (i.e. DSI already present in the card)                          |
| Le         | '00' or 'xx' = Length of expected digital signature                   |

**Table 21 — PSO: COMPUTE DS response**

|            |                                 |
|------------|---------------------------------|
| Data field | Digital signature               |
| SW1-SW2    | '9000' or specific status bytes |

#### 6.7.4 Selection of different algorithms and input formats

If the card supports several digital signature algorithms or different Digital Signature Input formats (e.g. according to PKCS #1 (default) and ISO/IEC 9796-2rnd (see annex A), then the algorithm or the DSI format has to be selectable with the MSE command according to DIN V 66291-1 (there are 2 ways described: selecting an SE or setting the AlgID; the first one is outlined in DIN V 66291-1, the latter one is outlined subsequently).

**Table 22 — MANAGE SECURITY ENVIRONMENT command for selection of signature algorithm or DSI**

|            |                                           |
|------------|-------------------------------------------|
| CLA        | As defined in ISO/IEC 7816-4 and -8       |
| INS        | '22' = MANAGE SECURITY ENVIRONMENT        |
| P1         | '41' = SET for computation                |
| P2         | 'B6' = DST (CRT for digital signature)    |
| Lc         | '03' = Length of subsequent data field    |
| Data field | '8001xx'<br>= DO for AlgID, see table A.1 |
| Le         | Empty                                     |

**Table 23 — MANAGE SECURITY ENVIRONMENT response**

|            |                                 |
|------------|---------------------------------|
| Data field | Empty                           |
| SW1-SW2    | '9000' or specific status bytes |

In a similar way a hash algorithm may be selected with the MSE command, if the card supports more than one type of hash function.

**Table 24 — MANAGE SECURITY ENVIRONMENT command for selection of hash algorithm**

|            |                                           |
|------------|-------------------------------------------|
| CLA        | As defined in ISO/IEC 7816-4 and -8       |
| INS        | '22' = MANAGE SECURITY ENVIRONMENT        |
| P1         | '41' = SET for computation                |
| P2         | 'AA' = HT (CRT for hash code)             |
| Lc         | '03' = Length of subsequent data field    |
| Data field | '8001xx'<br>= DO for AlgID, see table A.1 |
| Le         | Empty                                     |

**Table 25 — MANAGE SECURITY ENVIRONMENT response**

|            |                                 |
|------------|---------------------------------|
| Data field | Empty                           |
| SW1-SW2    | '9000' or specific status bytes |

### 6.7.5 Reading and Writing Protocol Records

First the file EF.PROT must be selected.

**Table 26 — SELECT FILE command to select the protocol file**

|            |                                     |
|------------|-------------------------------------|
| CLA        | As defined in ISO/IEC 7816-4 and -8 |
| INS        | 'A4' = SELECT FILE                  |
| P1         | '02' = EF file selection            |
| P2         | '0C' = No FCI to be returned        |
| Lc         | '02' = Length of data field         |
| Data field | FID of EF.PROT, see annex C         |
| Le         | Empty                               |

**Table 27 — SELECT FILE response**

|            |                                 |
|------------|---------------------------------|
| Data field | Empty                           |
| SW1-SW2    | '9000' or specific status bytes |

To read the last protocol record the READ RECORD command has to be used. See tables 28 and 29.

**Table 28 — READ RECORD command to read a protocol record**

|            |                                           |
|------------|-------------------------------------------|
| CLA        | As defined in ISO/IEC 7816-4 and -8       |
| INS        | 'B2' = READ RECORD                        |
| P1         | '01' = Record no. 1 (last written record) |
| P2         | '04' = Read record P1                     |
| Lc         | Empty                                     |
| Data field | Empty                                     |
| Le         | 'xx' = Length of record                   |

**Table 29 — READ RECORD response**

|            |                                 |
|------------|---------------------------------|
| Data field | Protocol data                   |
| SW1-SW2    | '9000' or specific status bytes |

Further protocol records can be read by setting the record number in P1 to a higher value.

To write a protocol record the APPEND RECORD command has to be used. See tables 30 and 31.

**Table 30 — APPEND RECORD command to write a protocol record**

|            |                                     |
|------------|-------------------------------------|
| CLA        | As defined in ISO/IEC 7816-4 and -8 |
| INS        | 'E2' = APPEND RECORD                |
| P1,P2      | '0000'                              |
| Lc         | 'xx' = Length of record             |
| Data field | Protocol data                       |
| Le         | Empty                               |

**Table 31 — APPEND RECORD response**

|            |                                 |
|------------|---------------------------------|
| Data field | Empty                           |
| SW1-SW2    | '9000' or specific status bytes |

### 6.7.6 Reading the Display Message

Signatures at a public customer service terminal require a mutual authentication with session key agreement for secure messaging (see annex D).

After the mutual authentication has been processed successfully according to clause 5.10, the commands SELECT FILE and READ BINARY must be used to read the display message (display text 8 bytes, ASCII coded) shown on the display, individually for each chipcard, so that the user also recognises that the mutual authentication was successful.

Access to the 'Display Message' is only allowed after successful mutual authentication.

NOTE 1 Confirmation of the message by the user is considered sensitive, although no interaction with the card follows.

The commands SELECT FILE and READ BINARY in the SM-Mode are structured as shown in tables 32 to 35.

**Table 32 — SELECT FILE command to select the EF.DM**

|            |                                                                            |
|------------|----------------------------------------------------------------------------|
| CLA        | '0C' = Command with SM                                                     |
| INS        | 'A4' = SELECT FILE                                                         |
| P1         | '02' = EF file selection                                                   |
| P2         | '0C' = No FCI to be returned                                               |
| Lc         | 'xx' = Length of subsequent data field                                     |
| Data field | '81 02 D0 00'    '8E'- L-'xx ... xx'<br>= PV-DO with FID of EF.DM    CC-DO |
| Le         | '00'                                                                       |

**Table 33 — SELECT FILE response**

|            |                                                             |
|------------|-------------------------------------------------------------|
| Data field | '99 02 90 00'    '8E'-L-'xx ... xx'<br>= Status-DO    CC-DO |
| SW1-SW2    | '9000' or specific status bytes                             |

**Table 34 — READ BINARY command to read the Display Message**

|            |                                                      |
|------------|------------------------------------------------------|
| CLA        | '0C' = Command with SM                               |
| INS        | 'B0' = READ BINARY                                   |
| P1,P2      | '0000'                                               |
| Lc         | 'xx' = Length of subsequent data field               |
| Data Field | '97 01 08'    '8E'-L-'xx ... xx'<br>= Le-DO    CC-DO |
| Le         | '00'                                                 |

**Table 35 — READ BINARY response**

|            |                                                            |
|------------|------------------------------------------------------------|
| Data field | '87'-L-'xx .. xx'    '8E'-L-'xx .. xx'<br>= CG-DO    CC-DO |
| SW1-SW2    | '9000' or specific status bytes                            |

NOTE 2 The command READ BINARY is also allowed after user authentication on private or company terminals. In this case SM is not applied.

### 6.7.7 Updating the Display Message

Changing the Display Message is only allowed after user authentication. It is done via the command UPDATE BINARY. See tables 36 and 37.

**Table 36 — UPDATE BINARY command to change the Display Message**

|            |                                                              |
|------------|--------------------------------------------------------------|
| CLA        | '0C' = Command with SM                                       |
| INS        | 'D6' = UPDATE BINARY                                         |
| P1,P2      | '0000'                                                       |
| Lc         | 'xx' = Length of subsequent data field                       |
| Data field | '87'-L-'xx ... xx'    '8E'-L-'xx ... xx'<br>= CG-DO    CC-DO |
| Le         | '00'                                                         |

**Table 37 — UPDATE BINARY response**

|            |                                                             |
|------------|-------------------------------------------------------------|
| Data field | '99 02 90 00'    '8E'-L-'xx ... xx'<br>= Status-DO    CC-DO |
| SW1-SW2    | '9000' or specific status bytes                             |

NOTE The command UPDATE BINARY is also allowed on private or company terminals. In this case SM is not applied.

## 6.8 Authentication with CV Certificates

### 6.8.1 CV Certificate Verification

Before performing the authentication procedure, the certificate  $C\_CV.ICC.AUT$  and possibly the certificate  $C\_CV.CA.CS-AUT_{ICC/IFD}$  read from the card before selecting the  $\overline{DF}.BSS$  has to be verified in the IFD. It is assumed that the

- $PK.RCA.CS-AUT_{ICC/IFD}$  and possibly the
- $PK.CA.CS-AUT_{ICC/IFD}$  is present in the IFD.

The real procedure from the viewpoint of the card starts with verifying the CV-certificate of the IFD. The public key of the CA for verification, i.e. the  $PK.CA.CS-AUT_{ICC/IFD}$  is expected to be in the card (if not, then this key has to be delivered in a CV certificate which can be verified with the  $PK.RCA.CS-AUT_{ICC/IFD}$  present in the card). For CV-certificate verification the following commands have to be performed:

- **MANAGE SECURITY ENVIRONMENT** for setting the public key of the CA (i.e.  $PK.CA.CS-AUT_{ICC/IFD}$ )
- **VERIFY CERTIFICATE** for checking the CV-certificate presented by the IFD.

**Table 38 — MSE command**

|            |                                                           |
|------------|-----------------------------------------------------------|
| CLA        | As defined in ISO/IEC 7816-4 and -8                       |
| INS        | '22' = MANAGE SECURITY ENVIRONMENT                        |
| P1         | '81' = SET for verification                               |
| P2         | 'B6' = DST (CRT for digital signature)                    |
| Lc         | '0A' = Length of subsequent data field                    |
| Data field | '8308 ...'<br>= DO for KeyRef of $PK.CA.CS-AUT_{ICC/IFD}$ |
| Le         | Empty                                                     |

**Table 39 — MSE response**

|            |                                 |
|------------|---------------------------------|
| Data field | Empty                           |
| SW1-SW2    | '9000' or specific status bytes |

After the  $PK.CA.CS-AUT_{ICC/IFD}$  is set, then the **VERIFY CERTIFICATE** command is sent whereby command chaining is used (for command chaining, see ISO/IEC 7816-8).

a) Certificate with signature giving message recovery

**Table 40 — PSO: VERIFY CERTIFICATE Command**

|            |                                                                                                                                                                     |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CLA        | '1x'                                                                                                                                                                |
| INS        | '2A' = PERFORM SECURITY OPERATION:<br>VERIFY CERTIFICATE                                                                                                            |
| P1         | '00'                                                                                                                                                                |
| P2         | 'AE' (= Certificate in the data field, signed<br>signature input consists of non-BER-TLV-<br>coded data, i.e. the certificate content is a<br>concatenation of DEs) |
| Lc         | Length of subsequent data field                                                                                                                                     |
| Data field | '5F37'-L-SIG.CA (see annex B)                                                                                                                                       |
| Le         | Empty                                                                                                                                                               |

**Table 41 — PSO: VERIFY CERTIFICATE Response**

|            |                                 |
|------------|---------------------------------|
| Data field | Empty                           |
| SW1-SW2    | '9000' or specific status bytes |

**Table 42 — PSO:VERIFY CERTIFICATE Command**

|            |                                                                                                                                                                     |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CLA        | '0x'                                                                                                                                                                |
| INS        | '2A' = PERFORM SECURITY OPERATION:<br>VERIFY CERTIFICATE                                                                                                            |
| P1         | '00'                                                                                                                                                                |
| P2         | 'AE' (= Certificate in the data field, signed<br>signature input consists of non-BER-TLV-<br>coded data, i.e. the certificate content is a<br>concatenation of DEs) |
| Lc         | 'xx'= Length of subsequent data field                                                                                                                               |
| Data field | '5F38'-L-PK-remainder (see annex B)                                                                                                                                 |
| Le         | Empty                                                                                                                                                               |

**Table 43 — PSO: VERIFY CERTIFICATE Response**

|            |                                 |
|------------|---------------------------------|
| Data field | Empty                           |
| SW1-SW2    | '9000' or specific status bytes |

- b) Certificate with signature not giving message recovery

**Table 44 — PSO: VERIFY CERTIFICATE command**

|            |                                                                                                                                                                   |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CLA        | '1x'                                                                                                                                                              |
| INS        | '2A' = PERFORM SECURITY OPERATION:<br>VERIFY CERTIFICATE                                                                                                          |
| P1         | '00'                                                                                                                                                              |
| P2         | 'AE' = Certificate in the data field, signed<br>signature input consists of non-BER-TLV-<br>coded data, i.e. the certificate content is a<br>concatenation of DEs |
| Lc         | 'xx' = Length of subsequent data field                                                                                                                            |
| Data field | '5F4E'-L-Certificate content (see annex B)                                                                                                                        |
| Le         | Empty                                                                                                                                                             |

**Table 45 — PSO: VERIFY CERTIFICATE response**

|            |                                 |
|------------|---------------------------------|
| Data field | Empty                           |
| SW1-SW2    | '9000' or specific status bytes |

**Table 46 — PSO: VERIFY CERTIFICATE command**

|            |                                                                                                                                                                   |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CLA        | '0x'                                                                                                                                                              |
| INS        | '2A' = PERFORM SECURITY OPERATION:<br>VERIFY CERTIFICATE                                                                                                          |
| P1         | '00'                                                                                                                                                              |
| P2         | 'AE' = Certificate in the data field, signed<br>signature input consists of non-BER-TLV-<br>coded data, i.e. the certificate content is a<br>concatenation of DEs |
| Lc         | 'xx' = Length of subsequent data field                                                                                                                            |
| Data field | '5F37'-L-CA signature (see annex B)                                                                                                                               |
| Le         | Empty                                                                                                                                                             |

**Table 47 — PSO: VERIFY CERTIFICATE response**

|            |                                 |
|------------|---------------------------------|
| Data field | Empty                           |
| SW1-SW2    | '9000' or specific status bytes |

## 6.8.2 Setting the Keys for Authentication

Before the INTERNAL/EXTERNAL AUTHENTICATE commands are performed the keys to be applied by the card for these commands have to be set.

**Table 48 — MSE command**

|            |                                                                                                                 |
|------------|-----------------------------------------------------------------------------------------------------------------|
| CLA        | As defined in ISO/IEC 7816-4 and -8                                                                             |
| INS        | '22' = MANAGE SECURITY ENVIRONMENT                                                                              |
| P1         | 'C1' = SET for int./ext. authentication                                                                         |
| P2         | 'A4' = AT (CRT for authentication)                                                                              |
| Lc         | 'xx' = Length of subsequent data field                                                                          |
| Data field | '830Cxx ...xx'    '840101'<br>= DO KeyRef of PK.IFD.AUT, i.e. ICCSN.IFD    DO KeyRef of SK.ICC.AUT, see table 2 |
| Le         | Empty                                                                                                           |

**Table 49 — MSE response**

|            |                                 |
|------------|---------------------------------|
| Data field | Empty                           |
| SW1-SW2    | '9000' or specific status bytes |

### 6.8.3 ICC/IFD Authentication

For ICC/IFD authentication (see annex D) the card has to perform the INTERNAL AUTHENTICATE command in a first step.

**Table 50 — INT. AUTHENTICATE command**

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

**Table 51 — INT. AUTHENTICATE response**

|            |                                                                                                                                                                                                                                                |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Data field | — for RSA: Digital signature (DSI format ISO/IEC 9796-2, see DIN V 66291-1, Table D.1: '6A'    PRND1    K1    h(PRND1    K1    RND.IFD    ICCSN.IFD, least significant 8 bytes)    'BC' with h = SHA-1)<br>— for other algorithms: see annex D |
| SW1-SW2    | '9000' or specific status bytes                                                                                                                                                                                                                |

After the card has been successfully authenticated, the commands

— GET CHALLENGE and

— EXTERNAL AUTHENTICATE

are sent to the card.

**Table 52 — GET CHALLENGE command**

|            |                                     |
|------------|-------------------------------------|
| CLA        | As defined in ISO/IEC 7816-4 and -8 |
| INS        | '84' = GET CHALLENGE                |
| P1, P2     | '0000'                              |
| Lc         | Empty                               |
| Data field | Empty                               |
| Le         | '08' = Length of expected RND       |

**Table 53 — GET CHALLENGE response**

|            |                                 |
|------------|---------------------------------|
| Data field | RND.ICC (8 bytes)               |
| SW1-SW2    | '9000' or specific status bytes |

After GET CHALLENGE the command EXTERNAL AUTHENTICATE follows, which delivers the digital signature of the IFD to the card.

**Table 54 — EXT. AUTHENTICATE command**

|            |                                                                                                                                                                                                                                                                                           |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CLA        | As defined in ISO/IEC 7816-4 and -8                                                                                                                                                                                                                                                       |
| INS        | '82' = EXTERNAL AUTHENTICATE                                                                                                                                                                                                                                                              |
| P1         | '00'                                                                                                                                                                                                                                                                                      |
| P2         | '00'                                                                                                                                                                                                                                                                                      |
| Lc         | 'xx' = Length of subsequent data field                                                                                                                                                                                                                                                    |
| Data field | Authentication related data:<br><br>For RSA: digital signature of IFD (DSI format ISO/IEC 9796-2, see DIN V 66291-1, table D.1: '6A'    PRND2    K2    h(PRND2    K2    RND.ICC    ICCSN.ICC, least significant 8 bytes)    'BC' with h = SHA-1)<br><br>For other algorithms: see annex D |
| Le         | Empty                                                                                                                                                                                                                                                                                     |

**Table 55 — EXT. AUTHENTICATE response**

|            |                                 |
|------------|---------------------------------|
| Data field | Empty                           |
| SW1-SW2    | '9000' or specific status bytes |

After successful authentication of the external entity the respective security status is set in the card.