

Identification card systems — European Citizen Card —

Part 2: Logical data structures and card services

ICS 35.240.15

National foreword

This Draft for Development was published by BSI. It is the UK implementation of CEN/TS 15480-2:2007.

This publication is not to be regarded as a British Standard.

It is being issued in the Draft for Development series of publications and is of a provisional nature. It should be applied on this provisional basis, so that information and experience of its practical application can be obtained.

Comments arising from the use of this Draft for Development are requested so that UK experience can be reported to the European organization responsible for its conversion to a European standard. A review of this publication will be initiated not later than 3 years after its publication by the European organization so that a decision can be taken on its status. Notification of the start of the review period will be made in an announcement in the appropriate issue of *Update Standards*.

According to the replies received by the end of the review period, the responsible BSI Committee will decide whether to support the conversion into a European Standard, to extend the life of the Technical Specification or to withdraw it. Comments should be sent to the Secretary of the responsible BSI Technical Committee at British Standards House, 389 Chiswick High Road, London W4 4AL.

The UK participation in its preparation was entrusted to Technical Committee IST/17, Cards and personal identification.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

This Draft for Development was published under the authority of the Standards Policy and Strategy Committee on 31 May 2007

© BSI 2007

ISBN 978 0 580 50659 8

Amendments issued since publication

Amd. No.	Date	Comments

English Version

Identification card systems - European Citizen Card - Part 2: Logical data structures and card services

Systèmes des cartes d'identification - Carte Européenne du
Citoyen - Partie 2: Structures logiques des données et
services cartes

Identifikationskartensysteme - Europäische Bürgerkarte -
Teil 2: Logische Datenstrukturen und Kartendienste

This Technical Specification (CEN/TS) was approved by CEN on 17 July 2006 for provisional application.

The period of validity of this CEN/TS is limited initially to three years. After two years the members of CEN will be requested to submit their comments, particularly on the question whether the CEN/TS can be converted into a European Standard.

CEN members are required to announce the existence of this CEN/TS in the same way as for an EN and to make the CEN/TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force (in parallel to the CEN/TS) until the final decision about the possible conversion of the CEN/TS into an EN is reached.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: rue de Stassart, 36 B-1050 Brussels

Contents

Page

Foreword.....	4
1 Scope	5
2 Normative references	5
3 Terms and definitions	6
4 Abbreviations	6
4.1 Abbreviations	6
4.2 Coding conventions and notation.....	8
5 Data elements and data structures	10
5.1 Supported data Structures	10
5.2 Access to data structures	10
5.3 Answer to reset (ATR) / answer to select (ATS)	11
5.4 General architecture and file supported	13
5.5 Selection of data structures	14
5.6 Access to files	14
6 Basic card services	16
6.1 General.....	16
6.2 Identification.....	16
6.3 User verification.....	17
6.4 Device authentication.....	18
6.5 Digital signature.....	21
6.6 Client/server authentication	24
6.7 Encryption key decipherment	24
7 Extended card services.....	24
7.1 General.....	24
7.2 Biometrics – on card matching	24
7.3 Passive authentication	25
7.4 Basic access control	25
7.5 Active authentication	25
7.6 Extended access control	25
7.7 Role authentication.....	25
Annex A (normative) Command set.....	27
A.1 CLASS byte coding.....	27
A.2 Command chaining mechanisms.....	27
A.3 Retrieval of response data longer than 256 bytes.....	28
A.4 Logical channels.....	28
A.5 Short and extended length fields	29
A.6 Status words	29
A.7 Command set	30
Annex B (normative) Card Verifiable Certificates	47
B.1 Introduction	47
B.2 Use of the public key extracted from the certificate	47
B.3 Validity of the key extracted from a certificate	47
B.4 Structure of CVC	47
B.5 Steps of CVC verification	48
B.6 Commands to handle the CVC	48
Annex C (normative) Cryptographic Information Application	49
C.1 Description	49
C.2 CIA data organisation.....	57

Annex D (normative) Mandatory and optional features	76
D.1 General	76
D.2 Data elements and data structures.....	76
D.3 Card services	77
D.4 Command set	78
D.5 Algorithms.....	79
Annex E (normative) Key and signature formats for elliptic curves over prime fields GF(p)	80
Annex F (informative) Access rules in expanded format.....	81
F.1 Object protection by access rules in expanded format	81
F.2 Access rules in expanded format	81
F.3 Security attribute referencing expanded format	82
F.4 Security attribute template for physical interfaces.....	83
Annex G (informative) Example of data structure: the Security Data Objects concept	84
G.1 SDO concept	84
Annex H (informative) Extended access control for MRTDs	98
H.1 General	98
H.2 Extended access control protocol.....	98
H.3 CV certificates for EAC	103
Bibliography	105

Foreword

This document (CEN/TS 15480-2:2007) has been prepared by Technical Committee CEN/TC 224 “Personal identification, electronic signature and cards and their related systems and operations”, the secretariat of which is held by AFNOR.

CEN/TS 15480, *Identification card systems — European Citizen Card* consist of the two following parts:

Part 1: *Physical, electrical and transport protocol characteristics*

Part 2: *Logical data structures and card services*

Part 3: *ECC Interoperability using an application interface*

Part 4: *Recommendations for ECC issuance, operation and use*

According to the CEN/CENELEC Internal Regulations, the national standards organizations of the following countries are bound to announce this CEN Technical Specification: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

1 Scope

This Technical Specification specifies the logical characteristics and security features at the card/system interface for the European Citizen Card.

The European Citizen Card is a smart card with Identification, Authentication and electronic Signature (IAS) services. Therefore:

- the supported services are specified;
- the supported data structures as well as the access to these structures are specified;
- the command set is defined.

This Technical Specification has the objective of ensuring the interoperability at card/system interface in the usage phase.

In order to reach the interoperability objective, IAS services are compliant to prEN 14890 part 1 and part 2. As the CWA documents offer options, this specification fully defines a complete profile. This specification also provides other features not defined in the CWA documents (biometric on card matching, command chaining, role authentication ...).

This Technical Specification is also compliant with ICAO specification (authentication methods, basic access control ...).

This Technical Specification does not mandate the use of a particular technology, and is intended to allow both native and Java card technologies.

This specification encompasses mandatory and optional features. Optional features make up a toolbox of modular options from which issuers can pick up the necessary protocols to fulfil the requisites of their use cases. Mandatory features are necessarily to be implemented for a smart card to be compliant to this Technical Specification. Two IAS-enabled smart cards issued by two different issuers, and compliant with this Technical Specification but implementing different modular options out of this Technical Specification, can interoperate with a terminal provided such a terminal supports both options. Therefore, interoperability requires a specific agreement between issuers/governments in order to determine which cross-border services are to be shared, and consequently which protocols are to be supported by the terminals in each country.

All the APDU commands described in this Technical Specification are in accordance with ISO/IEC 7816 part 4 or part 8. They are fully described here in order to provide the settings adopted by this specification and to prevent any ambiguity in case of several possible interpretations of the standards.

For physical, electrical and transport protocol characteristics, refer to CEN/TS 15480-1.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ANSI X9.63, *Public Key Cryptography For the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography*, January 8th 1999

prEN 14890-1:2007, *Application Interface for smart cards used as Secure Signature Creation Devices — Part 1: Basic requirements*

prEN 14890-2:2007, *Application Interface for smart cards used as Secure Signature Creation Devices — Part 2: Additional Services*

ISO/IEC 7816-3, *Identification cards — Integrated circuit cards — Part 3: Cards with contacts — Electrical interface and transmission protocols*

ISO/IEC 7816-4:2005, *Identification cards — Integrated circuit(s) cards — Part 4: Organization, security and commands for interchange*

ISO/IEC 7816-11, *Identification cards — Integrated circuit cards — Part 11: Personal verification through biometric methods*

ISO/IEC 7816-15, *Identification cards — Integrated circuit cards with contact — Part 15: Cryptographic information application*

ISO/IEC 9796-2, *Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Integer factorisation based mechanisms*

ISO/IEC 14443-4, *Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 4: Transmission protocol*

ISO/IEC 15946-2, *Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 2: Digital signatures*

ISO/IEC 19794-2, *Information technology — Biometric data interchange formats — Part 2: Finger minutiae data*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1

Application Dedicated File (ADF)

ADF is a Dedicated File (DF) with an Application Identifier (AID)

3.2

root

Master File MF in case of a native operating system, the applet instance having the default selection privilege in case of a Java card implementation

4 Abbreviations

4.1 Abbreviations

ADF	Application Dedicated File
AID	Application Identifier
AMB	Access Mode Byte
AT	Authentication Template
ATR	Answer to Reset
ATS	Answer to Select

BER	Basic Encoding Rules
BHT	Biometric Header Template
BIT	Biometric Information Template
CA	Certification Authority
CAR	Certification Authority Reference
CCT	Cryptographic Checksum Template
CED	Certificate Effective Date
CHA	Certificate Holder Authorisation
CHR	Certificate Holder Reference
CIA	Cryptographic Information Application
CPI	Certificate Profile Identifier
CRT	Control Reference Template
CT	Confidentiality Template
CV	Card Verifiable
CXD	Certificate Expiration Date
DES	Data Encryption Standard
DF	Dedicated File
DH	Diffie Hellman
DOCP	Data Object Control Parameters
DST	Digital Signature Template
ECDH	Elliptic Curve DH
ELC	Elliptic Curve Cryptosystem
ECDSA	Elliptic Curve Digital Signature Algorithm
EF	Elementary File
FCI	File Control Information
FCP	File Control Parameters
HT	Hash Template
IAS	Identification, Authentication and electronic Signature
ICC	Integrated Circuit Card

IFD	Interface Device
KAT	Control reference template for key agreement
LSB	Least Significant Byte
MAC	Message Authentication Code
MF	Master File
MSE	Manage Security Environment
OID	Object Identifier
PAN	Primary Account Number
PIN	Personal Identification Number
PK – DH	Public key – Diffie Hellman (asymmetric key base algorithm)
PSO	Perform Security Operation
RFU	Reserved for Future Use
RSA	Rivest Shamir Adleman
SDO	Security Data Object
SCB	Security Condition Byte
SE	Security Environment
SEID	Security Environment Identifier byte
SM	Secure Messaging
TLV	Tag Length Value
UQB	Usage Qualifier Byte

4.2 Coding conventions and notation

4.2.1 Coding conventions

The following coding conventions apply throughout the Technical Specification:

'0' to '9' and 'A' to 'F' the sixteen hexadecimal digits;

" ... " ASCII-string;

B1 || B2 concatenation of bytes B1 (the most significant byte) and B2 (the least significant byte).

4.2.2 Notation

For private and public keys as well as for certificates the following simplified Backus-Naur notation is used:

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

<key descriptor>::=	<asymmetric key>.<keyholder>.<usage>
<asymmetric key>::=	<private key> <public key>
<private key>::=	PrK
<public key>::=	PuK
<keyholder>::=	<cardholder> <device>
<cardholder>::=	CH
<device>::=	<integrated circuit(s) card> <interface device> <sender>
<integrated circuit(s) card>::=	ICC
<interface device>::=	IFD
<sender>::=	S
<usage>::=	<authentication> <role authentication> <key agreement> <key encipherment>
<authentication>::=	AUT
<key agreement>::=	KA
<role authentication>::=	RA
<key encipherment>::=	KE
<certificate descriptor>::=	<certificate>.<certholder>.<usage>
<certificate>::=	<card verifiable certificate> <X.509 certificate>
<card verifiable certificate>::=	C_CV
<X.509 certificate>::=	C_X509
<certholder>::=	<cardholder> <device>

EXAMPLES:

- 1) PrK.ICC.AUT = Private key of the ICC for device authentication;
- 2) PuK.S.KA = Public key of the sender used for key agreement;
- 3) C.CH.AUT = Certificate of the card holder for Client Server Authentication.

In addition the following notation is used:

K_{ICC}	Random number (32 bytes) of the ICC used for session key derivation
K_{IFD}	Random number (32 bytes) of the IFD used for session key derivation
K_{ENC}	Symmetric Key for encryption used in device and / or role authentication

K_{MAC}	Symmetric Key for MAC calculation used in device and / or role authentication
K_{SK-ENC}	Secure Messaging session key (3DES) for encryption
K_{SK-MAC}	Secure Messaging session key (3DES) for MAC calculation
RND.ICC	Random number (8 byte) of the ICC
RND.IFD	Random number (8 byte) of the IFD
SN.ICC	Serial number (8 LSB) of the ICC (IFD)
SN.IFD	Serial number (8 LSB) of the IFD

5 Data elements and data structures

5.1 Supported data Structures

The European Citizen Card shall support the data structures described in 5.2. These data structures are used to store external accessed data (certificates, card serial number, ...). Exceptions from this rule, i.e. use cases where data objects are used that can be accessed by a GET DATA command are listed in the description of the services.

In addition the card may support further data structures including proprietary structures to handle data as long as these structures have no effect on the services defined in this Technical Specification, i.e. on the interoperability. E.g. the storage of private and secret keys, the storage of PIN reference data and of security environments is not defined in this Technical Report. The storage of these entities is out of the scope of this Technical Specification and implementation specific.

5.2 Access to data structures

5.2.1 File system considerations

The European Citizen Card might embed a virtual machine or be a native operating system.

- 1) The card may include an MF. The differentiation between cards with or without an MF is based on the card ATR/ATS. See ISO/IEC 7816-4:2005, 8.1 – card service data byte. Consequently the card shall include the card service data byte when returning the ATR/ATS.
- 2) If an application is selected implicitly, i.e., always selected at the card reset, it has the default selection privilege. The corresponding AID shall be indicated in the historical bytes or the EF.ATR.
- 3) The root is the MF or the applet instance having the default selection privilege. This depends on the card manufacturer implementation choice (JavaCard or native implementation).
- 4) Three basic file types are supported:
 - i) transparent EF;
 - ii) dedicated files DF;
 - iii) application dedicated files ADF, refer to clause for a definition of the term ADF.
- 5) For card without MF, each applet instance matches with an application DF (ADF).

- 6) All cards shall be personalized with an EF.DIR file.
 - i) The EF.DIR is always under the root.
 - ii) The EF.DIR identifier is: '2F00', the short EF identifier is 30 = '1E' = 11110 bin.

5.3 Answer to reset (ATR) / answer to select (ATS)

5.3.1 General

The ATR of the card shall follow the rules indicated in ISO/IEC 7816-3 and ISO/IEC 7816-4. The ATS of the card shall follow the rules specified in ISO/IEC 14443-4.

Data objects for card identification shall be provided in the historical data bytes of the ATR/ATS or in an optional EF.ATR. If both ATR/ATS and EF.ATR specify data objects, the data objects from ATR/ATS shall be present in EF.ATR and optionally more data objects. In case of ISO/IEC 14443-4 and protocol type B no ATS is available and for this reason the presence of the EF.ATR is mandatory in this case.

Card Identification Data Objects table provides the list of data objects which may be supported by the card. The data objects are shown for the BER-TLV structure as used in an EF.ATR. For data objects transmitted in the historical data bytes the compact TLV format as defined in ISO/IEC 7816-4 shall apply.

If a data object format is used in the historical bytes or in EF.ATR the length of the DO shall be used as defined in the table. Furthermore the definitions for the coding of content of the data objects given in the table are mandatory. The coding of further parameters in the content of the data objects is left to the choice of the card manufacturer but shall follow the rules given in ISO/IEC 7816-4.

Table 1 — Card Identification Data Objects

Tag	Length	What	Content	Support
'43'	'01'	Card service data	Byte 1: b8=1: Application selection by full DF name b6=1: BER TLV DO are present in EF.DIR b4..b2=100: EF.DIR / EF.ATR is a transparent EF (use READ BINARY) b1=1: card with MF (i.e. Native card) b1=0 : card without MF (i.e. Java card)	Mandatory
'46'	'04'	Pre-issuing DO	Byte 1: IC Manufacturer according ISO/IEC 7816-6 Byte 2: Type of the IC, defined by the IC or card manufacturer Byte 3: Version of the operating system defined by card manufacturer Byte 4: Discretionary data (defined by the card manufacturer)	Optional
'47'	'03'	Card capabilities	Byte 1 (DF / EF selection): b8=1: DF selection by full name b5=1: DF selection using file identifier b3=1: file selection using short file identifier is supported Byte 2 (data coding byte): b4...b1 = 0001: data unit size is 1 byte Byte 3: b8=1: command chaining is supported b5, b4 = 00: No logical channel supported b5, b4 = 10: channel number assignment by the card Maximum number of channels supported: 4	Mandatory
'4F'	'01'...'10'	Application Identifier	AID of an implicitly selected application	Conditional: This DO shall be present if there is an implicitly selected application
'E0'	variable	IO buffer size	Four data objects with tag .02. (universal class). The value field of each DO encodes the maximum number of bytes of the respective APDU. .02. . L . .xx .xx. .02. . L . .xx .xx. .02. . L . .xx .xx. .02. . L . .xx .xx. = DO maximum length of command APDU without secure messaging DO maximum length of command APDU with secure messaging DO maximum length of response APDU without secure messaging DO maximum length of response APDU with secure messaging.	Conditional: This DO shall be present if the ECC platform supports extended length fields

5.3.2 Historical bytes

The category indicator as the first historical byte shall be set to the value '00'. Therefore the last three bytes shall be a status indicator, i.e. a card life cycle status indicator followed by two status bytes SW1-SW2.

Transmission in historical bytes for the data objects "card service data" and "card capabilities" is mandatory. For other data objects the decision is left to the card manufacturer.

5.3.3 EF.ATR

The usage of an EF.ATR is optional. The support of an EF.ATR shall be indicated in the "card service data byte" of the historical bytes. With regard to ISO/IEC 14443-4, the ATS Application information bytes are not normalized for data objects interoperable description. Therefore, for both contact and contact-less cards, EF.ATR may host information.

For data objects stored in the EF.ATR the BER-TLV format is mandatory.

5.4 General architecture and file supported

Figure 1 —shows an example of directory and elementary file organization.

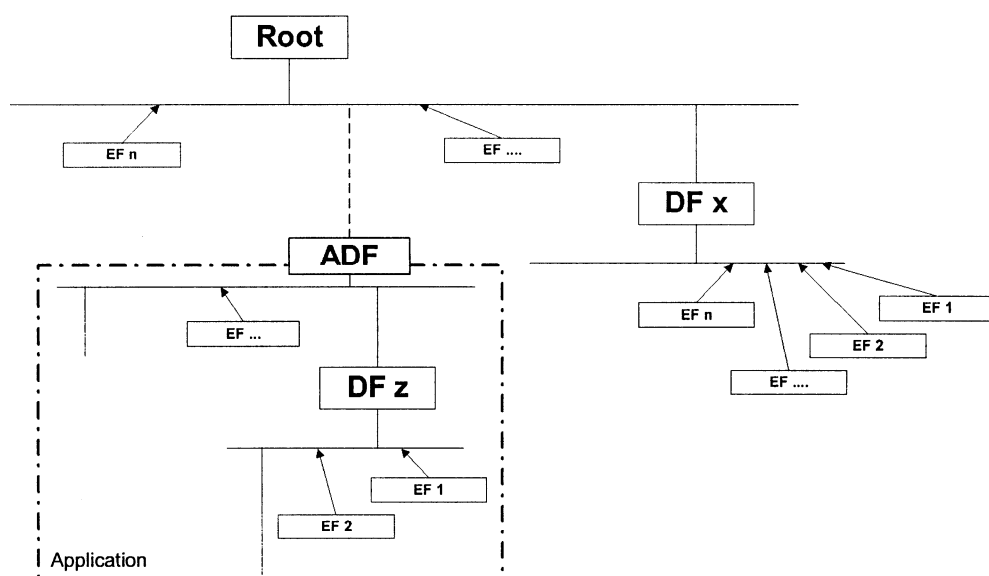


Figure 1 — Directory architecture example

The card supports the following type of files:

- the root is unique and identifies the default selected directory after reset;
- DF files that are attached to the root or to another DF;
- one or more ADFs each representing an application that may include dedicated files;
- transparent EF files.

An ADF may be stored under another ADF. Due to the fact that an ADF is always selected by its AID, this is not visible by the outside world.

For interoperability purpose, the European Citizen Card shall support at least one level of DF and ADF under the root and one level of DF under any ADF.

5.5 Selection of data structures

5.5.1 Selection of an application

After reset and return of the ATR/ATS, the root is automatically selected (refer to clause for definition of the root).

The terminal may select the EF.DIR, which is a mandatory EF, always present under the root. The EF.DIR is always selected by FID ('2F00') or addressed by its short EF identifier '1E' = 30.

The EF.DIR contains the list of the AID of the applications (ADF) present on the smart card.

ADF selection is always performed by name. An ADF may support the selection by more than one AID (e.g. a national and an international AID) in order to support interoperability.

In case of a card without MF (typically a Java card implementation), the SELECT by AID of an application shall be issued by the terminal always in clear, even if a secure messaging session is currently active. For such cards this SELECT by AID in clear shall not break the current secure messaging session (if any). For such cards this behaviour is necessary in order to allow the association of one applet instance to one application in a Java card.

5.5.2 Selection of files

File selection is always relative to the ADF. The EF selection can be performed either:

- explicitly by the SELECT command using FID over two bytes, or
- implicitly by addressing the file content using short EF identifier.

All files, except ADF or root (when card without MF), may be selected by file ID (2 bytes-long). An elementary file may also be selected implicitly by an access with short EF identifier.

5.6 Access to files

5.6.1 File control parameter

The File Control Parameter (FCP) referenced by tag '62' provides the logical, structural and security attributes of a file (EF or DF or ADF). Table 2 — File Control Parameter defines the subset of ISO/IEC 7816-4 to be supported at least by the ICC. The FCP is returned by a SELECT command if the corresponding command parameter is set, see Annex A. The European Citizen Card may return additional data objects in the FCP (i.e. data objects with other tags). Those data objects are to be ignored by the IFD in the context of ECC usage.

The ICC may also support File Control Information (FCI) and File Management Data (FMD) that may contain proprietary data not relevant with respect to interoperability. For this reason the FCI as well as the FMD are out of the scope of the present specification.

Table 2 — File Control Parameter

Tag	Length	Description			
'62'	Var.	File Control Parameter (FCP)			
		Tag	Length	Description	Applies to
		'80'	'02'	Number of data bytes in the file excluding structural information	Transparent EFs
		'82'	'01'	File descriptor byte (data coding byte)	DFs, ADFs, transparent EFs
		'83'	'02'	File Identifier coded on two bytes	DFs, transparent EFs ^a
		'84'	'01' to '10'	DF name (AID)	ADFfs
		'88'	'01'	Short EF identifier (optional)	EFs
		'8A'	'01'	Life cycle status byte	Any file
		'A1'	variable	Security attribute template for physical interfaces ^b	Any file
^a An ADF shall be selected by AID but the tag '83' may be present inside the FCP of an ADF. For interoperability reasons, an ADF shall not be selected by File ID.					
^b The patent situation has still to be clarified.					

Whether access rules in compact or in (referenced) expanded format compliant with ISO/IEC 7816-4 are supported is out of the scope of this Technical Specification.

In case an Application DF is selectable by more than one AID the FCP returned by a SELECT command shall contain at least the AID used to select the ADF.

The File Control Parameter data objects are encoded compliant with ISO/IEC 7816-4 and described in the following clauses.

There are no restrictions on file IDs, except for those defined by ISO (e.g. ID = '3F00' is reserved for the MF, '0000' is reserved for the current file, '3FFF' and 'FFFF' are forbidden etc.)

5.6.2 File descriptor byte

The file descriptor byte is encoded as defined in Table 3 — File descriptor byte. Bit 4, 5 and 6 are not relevant with respect to interoperability and therefore not defined in the present specification.

Table 3 — File descriptor byte

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0							File Accessibility Not shareable file
0	1							Shareable file
0	-	1	1	1	0	0	0	DF
0	-	Not all set to 1			-	-	-	EF category
0	-	-	-	-	0	0	1	EF structure Transparent structure
- 'Shareable' means that the file supports at least concurrent access on different logical channels. - The support of shareable files is optional.								

5.6.3 Life cycle status byte

Referenced by tag '8A' a life cycle status byte is present in the FCP of any file. This byte shall be interpreted compliant to ISO/IEC 7816-4 according to Table 4 — Life cycle status byte.

Table 4 — Life cycle status byte

b8	b7	b6	b5	b4	b3	b2	b1	Meaning	Applies to
0	0	0	0	0	0	0	1	Creation state ^a	Any file
0	0	0	0	0	0	1	1	Initialisation state ^a	Any file
0	0	0	0	0	1	-	1	Operational state (activated)	Any file
0	0	0	0	0	1	-	0	Operational state (deactivated)	Any file
0	0	0	0	1	1	-	-	Termination state	Any file
- Any other value is RFU									
^a Usage of creation and initialization states are implementation dependant.									

6 Basic card services

6.1 General

The card services described here from a functional standpoint relate to the IAS services as referred to in prEN 14890-1 and prEN 14890-2. Unless indicated OPTIONAL, the following services shall be supported.

6.2 Identification

6.2.1 Identification of the cardholder

At personalization time, any data dedicated to identify the cardholder are designated as identification data.

6.2.2 Identification of the European Citizen Card

If the European Citizen card makes use of the symmetric device authentication protocol according to clause 6.4.3 or an asymmetric device authentication protocol according to clause 6.4.4.2 or 6.4.4.3, the ECC shall

contain a Primary Account Number (PAN). The structure of the PAN is in accordance with ISO/IEC 7812-1 and defined in Table 5 — Primary Account Number. The PAN is BCD coded.

Table 5 — Primary Account Number

	ISO/IEC 7812 definition			
Length	6 digits (BCD)		12 digits (BCD)	1 digit (BCD)
Data	IIN Issuer Identification Number			Check digit
	MII	Country code	Issuer identifier	

For the Issuer Identification Number (IIN) the following definitions apply:

- Major Industry Identifier (MII) is a single digit with the value 9, i.e., for assignment by national standard bodies according to ISO/IEC 7812-1;
- country code is a three digit value in accordance with EN ISO 3166-1;
- issuer identifier is coded on two digits and identifies for the major industry and the country the card issuer in a unique way. The value is assigned by the corresponding national standard body.

The individual account identification is coded on 12 digits (BCD) and allows a unique identification of the smart card over all cards having the same IIN.

The check digit is a single digit and allows verification of the PAN integrity. The check digit is calculated according to the Luhn formula, see ISO/IEC 7812-1.

The PAN is stored in the elementary file EF.SN under the root. The contents of EF.SN is BER-TLV coded using the tag '5A' that references the PAN, see Table 6 — Structure of EF.SN. In this data object the PAN (19 digits) is concatenated with a filler digit (1 digit with value 'F', BCD encoded) in order to get a value field that is 10 bytes long. The (short) EF Identifier of EF.SN is provided by means of the Cryptographic Information Application.

Table 6 — Structure of EF.SN

Tag	Length	Value
'5A'	'0A'	PAN, (BCD encoded) Filler bit with value 'F'

Throughout the present specification the following elements of the concatenation of the PAN and the filler bit are used:

- rightmost 8 bytes are called smart card serial number SN.ICC and used in the context of the device authentication protocols;
- complete concatenation of the PAN and the filler bit is used in the Card Verifiable certificate of a European Citizen Card as Certificate Holder Reference (CHR), see Annex B.

6.3 User verification

6.3.1 General aspects

A retry counter and an initial value of the retry counter are defined for each reference data. If the verification fails, the retry counter is decremented by one and an error status that contains the remaining attempts is returned by the application.

When the retry counter equals zero, the reference data is blocked and can no longer be used. Note that a successful verification of the reference data resets its retry counter to the initial value.

The IAS platform supports a resetting code mechanism to unblock reference data, i.e. to reset the corresponding retry counter to its initial value and optionally to set new reference data. Whether resetting codes are supported or not and which command variant is supported is defined by the security attributes of the application as indicated in the corresponding DF.CIA.

6.3.2 Knowledge based

To insure interoperability:

- for the VERIFY command, the referenced data shall be encoded in the P2 parameter;
- for the CHANGE REFERENCE DATA command, the reference data shall be selected by a password reference encoded in the P2 parameter. Upon successful command execution the reference data inside the card is replaced by the new reference data provided in the command data field;
- for the RESET RETRY COUNTER, the referenced data shall be encoded in the P2 parameter.

NOTE Command flows for the VERIFY and the CHANGE REFERENCE DATA command can be found in the upcoming prEN 14890-1. Refer to A.7.5.7 for more information on the usage of the RESET RETRY COUNTER command.

6.3.3 Biometrics – on card matching

Please refer to 7.2.

6.4 Device authentication

6.4.1 General

The European Citizen Card shall at least implement one device authentication protocol based on asymmetric cryptography. For interoperability reasons a terminal shall implement all protocols based on asymmetric cryptography.

6.4.2 Authentication environments

Two kinds of environments shall be distinguished, by considering their security level: trusted and un-trusted environments. During the personalization phase, the issuer will define the access rules to the application resources. Different access rules can be defined for trusted and un-trusted environments. The terminal shall adapt the authentication to the security level required by the resource it wishes to access.

For definition of trusted/un-trusted environments, refer to prEN 14890-1:2007, 5.2 and 8.2.

6.4.3 Symmetric authentication scheme

The smart card implements the mutual authentication scheme using symmetric keys as defined in prEN 14890-1:2007, 8.8.

6.4.4 Asymmetric device authentication schemes

6.4.4.1 Card verifiable certificate verification commands

Card verifiable (CV) certificates are used in the context of asymmetric device authentication schemes to import a public key and related attributes into the European Citizen Card. The structure of the supported CV

certificates and the card internal verification process is specified in Annex B. Details about possible certification hierarchies can be found in prEN 14890-1:2007, Clause 8.

This clause defines the command flow used to verify a command chain.

6.4.4.2 Key transport protocol

The ICC makes use of the key transport protocol defined in prEN 14890-1:2007, 8.4 for an asymmetric device authentication service. This protocol makes use of card verifiable (CV) certificates, see Annex B of this Technical Specification, in order to import public keys into the ICC. Details about possible certification hierarchies and the calculation of the cryptographic authentication tokens can be found in the referenced document. While prEN 14890-1 offers several degrees of freedom with respect to the command syntax, this Technical Specification defines the commands to be used in detail in order to support interoperability.

AlgID DO in KAT CRT is mandatory.

6.4.4.3 Device authentication with privacy protection

The device authentication with privacy protection scheme is based on prEN 14890-1:2007, 8.5. To avoid the card disclosing private information, such as identity, a secure channel session is established before any other operation. To do so, the protocol starts with an unauthenticated Diffie-Hellman key exchange and then authenticates the IFD before the ICC.

Five main phases may be distinguished:

- 1) set the privacy protection;
- 2) transport of the IFD public key to the ICC;
- 3) external authentication of the IFD;
- 4) transport of the ICC public key to the IFD;
- 5) internal authentication of the ICC.

6.4.4.4 Privacy constrained device authentication with non traceability based on ELC

The protocol is constructed to serve special case of non-traceability. The protocol does not offer the amount of privacy as available in authentication with privacy protection (clause 6.4.4.3).

This protocol hinders a verifier to submit the provable existence of the verification process. A possible application is the use with contact less implementations in the context of citizen cards and homeland security. It enhances the existing EAC protocol by aspects of privacy.

Five main phases may be distinguished:

- Read public parameters;
- IFD authentication (EXTERNAL AUTHENTICATE);
- ICC authentication (INTERNAL AUTHENTICATE);
- Establish secure session;
- Verification of ICC's certificate.

6.4.5 Session key computation

Two 16-byte TDES session keys are required for the secure messaging protocol. These keys are derived from K_{IFD} and K_{ICC} during the device authentication protocol:

A this point the actual session keys shall be built from KIFD/ICC according to prEN 14890-1:2007, 8.8.

6.4.6 Send Sequence Counter (SSC) initialisation

The Send Sequence Counter is an 8-byte number that is initialised immediately after successful device authentication. The SSC is initialised and handled as specified in prEN 14890-1.

6.4.7 Secure messaging

6.4.7.1 General

Secure messaging session establishment begins with an IFD/ICC mutual authentication. SM session keys are computed during this mutual authentication step. The ECC platform shall support secure messaging; whether it is used depends on the use case.

The following is mandatory:

- an SM session always includes data confidentiality AND integrity. Data confidentiality only, or data integrity only are not supported;
- SM policy for incoming data and outgoing data shall be the same.

6.4.7.2 SM Data Objects

Ref prEN 14890-2:2007 clause 9.2

6.4.7.3 Treatment of secure messaging errors

Ref prEN 14890-1:2007 clause 9.3

For ending a secure session refer to prEN 14890-1:2007 clause 8.12.2

- status bytes of the card application may be sent along with SM DOs. In this case the SM session is not aborted by the card;
- status bytes other than defined above for SM errors may be sent without SM DO. In this case the behaviour of the card concerning the deletion of SM session keys is not defined by this Technical Specification.

6.4.7.4 Commands and responses under SM

Ref. prEN 14890-1:2007 clause 9.6

6.4.7.5 SM session breaking events

The SM session is handled acc. to prEN 14890-1:2007 clause 8.12.2

- Further exceptions are outlined in 5.5.1.

6.5 Digital signature

6.5.1 General

The European Citizen Card platform shall support at least one of the following two cryptographic algorithms for the digital signature service:

- RSA;
- ECDSA in accordance with ISO/IEC 15946-2 using elliptic curves over prime fields GF(p).

For further details refer to prEN 14890-1:2007 clause 7.

6.5.2 Hashing

The European Citizen Card shall support partial data hashing algorithm with last round processed by the card. In this case the IFD calculates the hash over the beginning of the data to sign and the ICC ends by finishing the hash calculation on the last block. In addition the card supports complete hashing of a byte string that is shorter than the block length of the hash algorithm.

The result is temporarily stored in the card until the next command execution that is PSO:COMPUTE DIGITAL SIGNATURE.

For further description refer to prEN 14890-1:2007 clause 7.3.

For a list of supported algorithm refer to prEN 14890-1:2007 clause 13.1 Table 13-1. Annex D defines the algorithms that are mandatory and optional to support.

6.5.3 Digital signature

The ECC shall comply with Table D-5.

Table C.13 — List of supported digital signature algorithms defines the algorithms and the corresponding algorithm identifier used in this specification. Annex D defines the algorithms that are mandatory and optional to support.

In the case of ECDSA the digital signature is calculated according to ISO/IEC 15946-2. Details on the PSO:COMPUTE DIGITAL SIGNATURE command can be found in Annex A.

Examples for RSA_SHA_PKCS1 signature steps:

- DER encoding of the hash code specified in a previous PSO-Hash command:

```
digestInfo ::= SEQUENCE {
    digestAlgorithm AlgorithmIdentifier of SHA-1,
    digest OCTET STRING
}
```

The exact sequence coding is according to prEN 14890-1:2007 clause 13.3.3 Table 13.11

- PKCS#1 padding on the obtained DER encoded;
- RSA signature (with the private key) of the obtained block;

- in case of PKCS#1 with SHA-256 the DigestInfo is coded as follows:
 - digital signature: PKCS#1 V1.5 with SHA-256
 - The DigestInfo bloc in the signature will be coded as per prEN 14890-1:2007 clause 13.3.3 Table 13.13

The command sequence is the following one:

Notation:

M Message to sign

H' denotes the length of the intermediate hash value in bytes

C' denotes the length of the counter indicating the number of bits already hashed in bytes

B denotes the block length of the hash algorithm in bytes

Table 20 — Digital signature

IFD				ICC
Partial hash calculation over M				
- HASH context setting (ref. prEN 14890-1 clause 7.5.2 Table 7-13) - MSE - P1='41', - P2='AA', (Lc = CRT HT length) - Data= CRT HT			→ ←	Set incoming CRT HT in the current SE
Tag	L	Value		
'80'	'01'	' XX' = hash algorithm		
- Smart card private key selection prior to the digital signature calculation (ref. - prEN 14890-1 clause 7.5.3 Table 7-15) - MSE - P1 = '41', - P2 = 'B6', (Lc = CRT DST length) - Data = CRT DST ('80'-'01'-'xx' '84'-'01'-'xx' = DO algorithm ID DO key reference)			→ ←	Set incoming CRT DST in the current SE, including the private key selection.
- Send partial hash data and require final hash round calculation. (ref. prEN 14890-1 clause 7.4.2 Table 7-3) - PSO - P1 = '90' // Hash - P2 = 'A0' // Incoming data for hash calculation - Data =			→	The card initializes the hashing context with incoming data resulting from the partial hash calculation, then ends the hash over the last data block.
Tag	Length	Value	←	
'90'	H'+C'	Intermediate hash value [H' long] concatenated with number of bits already hashed		
'80'	Var. (≤B')	Last block, to be hashed by the card		
Signature calculation (ref. prEN 14890-1 clause 7.4.2 Table 7-5)				
- PSO - P1 = '9E' // Signature - P2 = '9A' // data to sign - Data = N/A			→ ←	The card calculates the signature according to the current SE CRT DST and returns the result.

6.6 Client/server authentication

The European Citizen Card platform shall support at least one of the following two cryptographic algorithms for the Client Server Authentication service:

- RSA;
- ECDSA in accordance with ISO/IEC 15946-2 using elliptic curves over prime fields $GF(p)$.

The use case for the CSA service is described in detail in prEN 14890-2:2007 clause 6. In case of RSA the ICC computes a signature using a message digest as input according to prEN 14890-2. In case of ECDSA the ICC computes a signature using a hash value as input in accordance with reference [2] and [3] of the bibliography. For the client/server authentication, the INTERNAL AUTHENTICATE command is used.

6.7 Encryption key decipherment

6.7.1 General

The European Citizen Card platform shall support at least one of the following two cryptographic algorithms for the Encryption Key Decipherment service:

- RSA;
- ECDH in accordance with ANSI X9.63 using elliptic curves over prime fields $GF(p)$.

The use case for the Encryption Key Decipherment service is described in detail in prEN 14890-2:2007 clause 8.2 for RSA and clause 8.3 for DH. The use case for ECDH is in principal analogous to the DH case as discussed below.

6.7.2 Preceding steps

Preceding steps that are application specific, e.g. a user verification, are performed. The precondition for the usage of the service shall be defined in the corresponding Cryptographic Information Application.

If the IFD does not already have the ICC's Encryption Key Decipherment certificate denoted as C.CH.KE, the IFD reads the certificate from the transparent file EF_C.CH.KE. The (short) EF identifier is provided by means of the corresponding Cryptographic Information Application.

7 Extended card services

7.1 General

The extended card services described here from functional standpoint relate either to the ICAO requirements or to other services. Unless indicated OPTIONAL, the following services shall be supported.

7.2 Biometrics – on card matching

7.2.1 General

The support of biometric user verification (on-card matching) is optional. On-card matching (MOC) is provided only as a service to access on-card data or functions. On-card matching can be used in the same way as a PIN to set a card internal security status. It shall not be used to set a card external security status (for physical access etc.). In the latter case some information is required by the IFD about the quality of the matcher.

7.2.2 General aspects

If this service is supported, the Finger Minutiae Matcher compliant to ISO/IEC 19794-2 shall be used. The compact size finger minutiae format identified by the CBEFF format type '0005' shall be applied as encoding format for finger minutiae.

The ICC shall provide the IFD with information about the supported biometric verification service using a Biometric Information Template (BIT) compliant to ISO/IEC 7816-11 that shall be encoded as presented in prEN 14890-2:2007 clause 6.2.1

The enrolment process is out of the scope of the present specification.

Verification flow For verification with sensor off-card refer to prEN 14890-2:2007 clause 6.2.2.1

7.3 Passive authentication

OPTIONAL. Refer to ICAO 9303, Parts 1 to 3, requirements.

7.4 Basic access control

OPTIONAL. Refer to ICAO specifications.

7.5 Active authentication

OPTIONAL. Refer to ICAO specifications.

7.6 Extended access control

OPTIONAL. Refer to Annex H

7.7 Role authentication

7.7.1 General

These features are optional.

This clause presents the procedure to authenticate an external entity to the card in order to associate to it a specific role (e.g. access rights). The IAS platform supports these two mechanisms:

- symmetric role authentication (external authentication);
- asymmetric role authentication.

7.7.2 Symmetric external authentication

7.7.2.1 General

The following procedure describes:

- cryptographic operation that allow the authentication;
- specification of the associated role in the card.

7.7.2.2 Protocol

Refer to prEN 14890-2:2007 clause 7.3

7.7.2.3 Role description

The card implicitly knows the role associated with the KeySet. Prior to granting privileges associated with the role, the card validates the cryptogram delivered by the IFD as described above.

The identification of the role allows limited operation on files as described in 5.6.

In case the IFD addresses an MSE SET command conveying a CRT AT template within which the KeySet reference is nested, the card-application implicitly knows the role associated with this KeySet.

7.7.3 Asymmetric authentication

7.7.3.1 General

Public keys are transported through Card Verifiable Certificates (CVC) which are fully described in Annex B.

7.7.3.2 Protocol based on RSA

Refer to prEN 14890-2:2007 clause 7.4.1

7.7.3.3 Role description

The roles associated with the key are mapped in the CHA field, more precisely in the RoleID field. The whole CHA, including its RoleID part, has to be validated. For Role description details refer to prEN 14890-1:2007 clause 14.9.5

Annex A (normative)

Command set

A.1 CLASS byte coding

Table A.1 — Interindustry values of CLA

b8	b7	b6	b5	b4	b3	b2	b1	Meaning	Support
0	0	0	X	-	-	-	-	Command chaining control	
			0	-	-	-	-	— The command is the last or only command of a chain	Mandatory
			1	-	-	-	-	— The command is not the last command of a chain	Mandatory
			-	X	X	-	-	Secure messaging indication	
			-	0	0	-	-	— No SM or no indication	Mandatory
			-	0	1	-	-	— Proprietary SM format	Out of scope
			-	1	0	-	-	— SM, command header not processed	Out of scope
			-	1	1	-	-	— SM, command header authenticated	Mandatory
			-	-	-	X	X	Logical channel number from zero to three	Optional

A.2 Command chaining mechanisms

A.2.1 Command chaining over incoming bytes

If indicated for a command in the present clause, command chaining shall be supported compliant to ISO/IEC 7816-4 as follows:

- smart card shall indicate the support of this mechanism in the historical bytes by means of the third software function table, see 5.3;
- CLA byte of the last command of a chain shall be coded as '0X', whereas all preceding commands shall be coded as '1X', see A.1;
- bit b1 to b4 of the CLA byte shall be identical for all commands of a chain;
- INS byte is identical in all commands of a chain. If P1 and / or P2 shall be identical as well, this is defined in the specification of the command;
- if a command is aborted, the execution of command chaining is aborted altogether;
- if a command chaining command with CLA '1X' is followed by a reset or a command that is not part of the chain, command chaining is aborted;
- if the smart card does not respond with status words SW1-SW2 set to '90 00' to a command of a chain with CLA '1X', command chaining is aborted;

- every command of a chain evaluates access rules separately and is secured by secure messaging separately, if secure messaging is to be applied. In case secure messaging is applied, the Send Sequence Counter (SSC) is incremented prior to every MAC verification of every command of the chain and prior to every MAC calculation of every response of the chain.

A.3 Retrieval of response data longer than 256 bytes

A.3.1 Use cases

In the following use cases the European Citizen Card shall be able to return at least 256 bytes plain data plus secure messaging bytes, so that the total length of the response data is longer than 256 bytes:

- usage of the PSO: COMPUTE DIGITAL SIGNATURE command with a sufficient key length and secure messaging;
- usage of INTERNAL AUTHENTICATE for Client Server Authentication with a sufficient key length and secure messaging;
- usage of READ BINARY with sufficient response data and secure messaging. If the terminal requests e.g. 256 bytes plain data by means of the Le = '00' byte and secure messaging is applied.

The following clauses define how these cases shall be treated.

A.3.2 Byte transmission protocol T = 0

The card makes use of the GET RESPONSE command with an interindustry value of the CLA byte '0x', see A.7.7.1.

The number of bytes available is indicated by the status words of the command that generated the response data, see A.6.

A.3.3 Byte transmission protocol T = 1

If the European Citizen Card indicates in the ATR/ATS that both protocol T=1 and extended length are supported, the IFD shall make use of extended length for the use cases defined in A.3.1.

The European Citizen Card behaviour for protocol T=1 and short APDU length fields as well as for protocol T=0 and short APDU length fields (A.3.2) in these use cases is according to this Technical Specification.

A.4 Logical channels

The European Citizen Card supports up to 4 logical channels as an optional feature. If the support of logical channels is indicated in the historical bytes of the ATR/ATS, the implementation shall be compliant to the present specification. Cards not supporting this mechanism shall make use of the basic channel with channel number zero only.

If the European Citizen Card supports logical channels, the number shall be indicated by means of the third software function table in the historical bytes of the ATR/ATS, see 5.3.

For referring to logical channels in the interindustry class the following rules that are compliant to ISO/IEC 7816-4 apply:

- CLA byte encodes the channel number from 0 to 3 of the command-response pair, see A.1;

- basic channel (channel number zero) shall be permanently available, i.e., it cannot be closed;
- after a RESET of the European Citizen Card the logical channels one to three are closed;
- channels other than the basic channel shall be opened by completion of the MANAGE CHANNEL command, see A.7.2.2, with open function;
- channels other than the basic channel shall be closed by completion of the MANAGE CHANNEL command, see A.7.2.2, with close function. After closing the channel shall be available for re-use;
- only one channel shall be active at a time;
- file descriptor byte defines for every EF or (Application) DF whether more than one channel may be opened to the same structure.

Each logical channel has its own security status. A security status shall not be shared between different logical channels.

A.5 Short and extended length fields

The handling of short and extended length fields shall be compliant to ISO/IEC 7816-4:

If the European Citizen Card states its capability of handling extended L_c and L_e fields in the third software function table of the historical bytes, then the card handles both extended and short length fields. Otherwise the card handles short length field only. In addition a card supporting extended length fields shall indicate the maximum number of bytes expected in the command data field by means of the ATR/ATS, see 5.3.

In any command response pair comprising both L_c and L_e fields short and extended length fields shall not be combined: either both of them are short or both of them are extended.

A.6 Status words

In general, status words shall be compliant to ISO/IEC 7816-4, but the actual values used are out of the scope of the document if not listed in the command description of this annex. In the command description only status words used in the user verification service with a meaning for the cardholder are mandated.

The following status words shall be used in the Secure Messaging protocol compliant to ISO/IEC 7816-4, prEN 14890-1 and the ICAO PKI report:

- '69 87' – Expected Secure Messaging data objects missing;
- '69 88' – Secure Messaging data objects incorrect;

The status words listed in the ICAO PKI report shall be used if the European Citizen Card hosts an MRTD application.

If byte transmission protocol $T = 0$ is applied the number of bytes to be retrieved by one or more consecutive GET RESPONSE commands shall be indicated by the status words:

- '61 00' if more than 255 bytes are available;
- '61 xx' where 'xx' indicates the number of bytes available.

A.7 Command set

A.7.1 General

NOTE Without loss of generality all command specifications are provided in the following for short APDU length fields only, but not for extended length fields. Instead of $L_e = '00'$ the ECC shall also be able to handle a concrete value.

A.7.2 Commands for selection

A.7.2.1 SELECT

The following tables define the variants of the SELECT command that are mandatory, optional and conditional to support.

Table A.2 — SELECT command-response pair

Command Parameter	Meaning
CLA	'0x', see Table A.1 — Interindustry values of CLA
INS	'A4'
P1	See Table A.3 — P1
P2	See Table A.4 — P2
L_C field	Absent or length of command data field
Data field	Absent or file identifier or DF name (according to P1)
L_e field	absent ($P2 = '0C'$) or '00'

Response Parameter	Meaning
Data field	Absent or file control information
SW1-SW2	See ISO/IEC 7816-4

The parameter $P1 = '00'$ shall be supported if the card indicates in the ATR/ATS that an MF is available.

The parameter $P1 = '09'$ shall be supported if the card indicates in the ATR/ATS that no MF is available.

Table A.3 — P1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning	Command data field	Support
0	0	0	0	0	0	X	X	Selection by file identifier		
				0	0	0	0	— Select MF	Absent	conditional
				0	0	0	1	— Select child DF	DF identifier	mandatory
				0	0	1	0	— Select EF under the current DF	EF identifier	mandatory
				0	0	1	1	— Select parent DF of the current DF	Absent	mandatory
				0	1	X	X	Selection by DF name		
				0	1	0	0	— Select by DF name	AID	mandatory
				1	0	X	X	Selection by path		
				1	0	0	1	— Select from the current DF	Path without the current DF identifier	conditional

Table A.4 — P2

b8	b7	b6	b5	b4	b3	b2	b1	Meaning	Support
0	0	0	0	-	-	X	X	File occurrence	
				-	-	0	0	— First or only occurrence	Mandatory
				X	X	-	-	File control information	
				0	0	-	-	— Return FCI template	Optional
				0	1	-	-	— Return FCP template	Mandatory
				1	1	-	-	— No response data, L _e byte absent	Mandatory

A.7.2.2 MANAGE CHANNEL

The support of the MANAGE CHANNEL command is conditional. If the card indicates in the historical bytes of the ATR/ATS that logical channels are supported, the implementation shall be compliant to the present specification.

When completed the command opens or closes a logical channel other than the basic one, i.e. a channel numbered from one to three.

The open function opens a logical channel other than the basic one. The channel number is assigned by the card and provided in the response data field, see Table A.5 — MANAGE CHANNEL command-response pair. After an open function is performed from the basic logical channel the root is selected, after an open function performed from a non-basic logical channel, the current DF on the channel numbered in CLA shall become current on the new channel. If the file descriptor byte of a DF indicates that the DF is not shareable, no further logical channel can be opened in this DF. The Security Environment of the logical channel is in the same state as after RESET, no security status is set in the opened channel.

The close function closes a logical channel other than the basic one. After closing, the channel shall be available for re-use. The channel to be closed is denoted in the P2 parameter byte, see Table A.5 — MANAGE CHANNEL command-response pair.