SLOVENSKI STANDARD
SIST-TS CEN/TS 15480-2:2009

01-februar-2009

Sistemi z identifikacijskimi karticami - Kartica evropskih drţavljanov - 2. del: Logiļne strukture podatkov in storitve v zvezi s kartico

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

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

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

Ta slovenski standard je istoveten z: **CEN/TS 15480-2:2007**

ICS:

35.240.15	Identifikacijske kartice in sorodne naprave	Identification cards and related devices

SIST-TS CEN/TS 15480-2:2009 **en**

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN/TS 15480-2

April 2007

ICS 35.240.15

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

Ref. No. CEN/TS 15480-2:2007: E

Contents

Page

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.

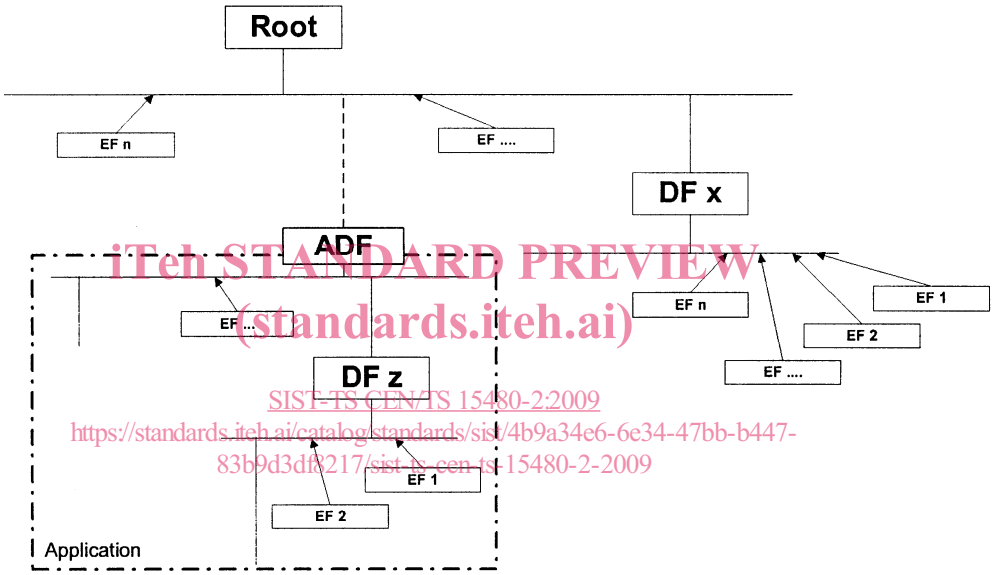

Figure 1 — Directory architecture example

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.