SLOVENSKI STANDARD

SIST-TS CEN/TS 15480-2:2012

01-september-2012

Nadomešča:

SIST-TS CEN/TS 15480-2:2009

Sistemi z identifikacijskimi karticami - Kartica evropskih državljanov - 2. del: Logične strukture podatkov in storitve v zvezi z varnostjo

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

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

Systèmes de cartes d'identification - Carte Européenne du Citoyen - Partie 2: structures de données logiques et services de sécurité

Ta slovenski standard je istoveten z: CEN/TS 15480-2:2012

ICS:

35.240.15	Identifikacijske kartice in sorodne naprave	Identification cards and related devices

SIST-TS CEN/TS 15480-2:2012 en,fr,de

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN/TS 15480-2

June 2012

ICS 35.240.15

English Version

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

Systèmes de cartes d'identification - Carte Européenne du Citoyen - Partie 2: structures de données logiques et services de sécurité

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

This Technical Specification (CEN/TS) was approved by CEN on 9 January 2012 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, Croatia, 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, Turkey and United Kingdom.

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

Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. CEN/TS 15480-2:2012: E

Contents

Page

Foreword

This document (CEN/TS 15480-2:2012) 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.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

This document supersedes CEN/TS 15480-2:2007.

CEN/TS 15480 *Identification card systems — European Citizen Card* consists of the following four parts:

Part 1, Physical, electrical and transport protocol characteristics

Part 2, Logical data structures and card services

Part 3, European Citizen Card Interoperability using an application interface

Part 4, Recommendations for European Citizen Card issuance, operation and use

According to the CEN/CENELEC Internal Regulations, the national standards organisations of the following countries are bound to announce this Technical Specification: Austria, Belgium, Bulgaria, Croatia, 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, Turkey and the 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 aims to ensure the interoperability at card/system interface in the usage phase.

In order to reach the interoperability objective, IAS services are compliant with EN 14890 Part 1 and Part 2. As the EN documents offer options, this specification fully defines a complete profile.

This Technical Specification also considers ICAO Doc 9303.

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 requirements for use. Mandatory features shall be implemented for a smart card to be compliant with this Technical Specification. Mandatory features required for compliancy to ECC specification are given in Annex C, the optional features are given in Annex D. Two IAS-enabled smart cards issued by two different issuers, and compliant with this Technical Specification but implementing different application profiles out of this Technical Specification, can interoperate with a terminal provided that such a terminal supports both application profiles. 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 documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

EN 14890-1:2008:2008, *Application Interface for smart cards used as Secure Signature Creation Devices — Part 1: Basic requirements*

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

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

ISO/IEC 7816-4:2005/PDAM 2.1:2008, *Identification cards — Integrated circuit(s) cards — Part 4: Organisation, security and commands for interchange, AMENDMENT 2: Handling of Extended Length Information (Working Draft)*

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 7816-15:2004/Amd 1:2007, *Identification cards — Integrated circuit cards with contact — Part 15: Cryptographic information application, AMENDMENT 1: Examples of the use of the cryptographic information application*

ISO/IEC 7816-15:2004/Amd 2:2008, *Identification cards — Integrated circuit cards with contact — Part 15: Cryptographic information application, AMENDMENT 2: Error corrections and extensions for multi-application environments*

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

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

BSI TR-03110 Version 1.11, *Advanced Security Mechansims for Machine Readable Travel Documents – Extended Access Control (EAC)*

BSI TR-03111 Version 1.11, *Technical Guideline Elliptic Curve Cryptography*

ICAO Doc 9303, Machine Readable Travel Documents, Part 3 – Machine Readable Official Travel Documents – Volume 2 Specifications for Electronically Enabled MRtds with Biometric Identification Capability, Third Edition, 2008

3 Terms and definitions

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

3.1
Application Dedicated File (ADF)
structure hosting an application in a card

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_X509.CH.AUT = Certificate of the card holder for client/server authentication.

In addition, the following notation is used:

$K_{ICC/IFD}$	Randomness provided by ICC and IFD used for session key derivation
RND.ICC	Random number of the ICC
RND.IFD	Random number of the IFD
SN.ICC	Serial number of the ICC
SN.IFD	Serial number 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 externally accessed data (certificates, card serial number, ...). Exceptions from this rule, i.e. 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. For example, 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 or the content of EF.ATR/INFO. 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 (native or JavaCard implementation).

4) Three basic file types are supported (refer to ISO/IEC 7816-4 for definitions of EF, DF and ADF):

i) transparent EF;

ii) dedicated files DF;

iii) application dedicated files ADF

5) For cards without MF, each applet instance matches with at least one application DF (ADF).

6) All cards shall contain an EF.DIR file.

i) The EF.DIR is always under the root.

ii) The file identifier of EF.DIR 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/INFO (see, 5.3.3). 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/INFO is mandatory in this case.

Table 1 provides the list of data objects which may be supported by the card in the ATR/ATS in the Compact-TLV format as defined in ISO/IEC 7816-4, Table 2 provides the data objects in EF.ATR/INFO for the BER-TLV structure. The data objects defined in Table 1 and Table 2 have to be used as given in the tables, these are not application specific.

5.3.2 Historical bytes

The ATR/ATS contains configuration data so that ICC and IFD can communicate together (protocol, speed, etc.).

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.

If a data object from Table 1 is used in the historical bytes 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 Historical Bytes

Byte #	Name	Value	Description
1	Category indicator	‘00’	COMPACT-TLV data objects followed by a status indicator shall be present as the last three historical bytes
2	Card service data tag	‘31’	Tag for next byte

3	Card service data byte	’B9’ or ‘B8’	b8=1: Application selection by full DF name
			b6=1: BER-TLV DO are present in EF.DIR
			b5=1: BER-TLV DO present in EF.ATR/INFO[a]
			b4...b2=100: EF.DIR/EF.ATR is a transparent EF (use READ BINARY)
			b1 = 0: Card with MF
			b1 = 1: Card without MF

4	Pre-issuing DO tag	‘64’	Tag for next 4 bytes
5	IC manufacturer	‘XX’	IC Manufacturer according ISO/IEC 7816-6
6	Type of the IC	‘XX’	defined by the IC or card manufacturer
7	OS Version	XX	Version of the operating system defined by card manufacturer
8	Discretionary data	‘XX’	Discretionary data
9	Card capabilities data tag	‘73’	Tag for next 3 bytes
10	Card capabilities data byte 1 → *Selection method*	‘94’	DF selection b8=1: DF selection full name b5=1: DF selection using file identifier EF selection b3=1: file selection using short file identifier is supported
11	Card capabilities data byte 2 → *Data coding byte*	‘01’	b4...b1 = 0001: data unit size is 1 byte
12	Card capabilities data byte 3 → *Miscellaneous*	‘C0’, ‘80’, ‘D0’ or ‘90’	b8=1: command chaining is supported b7=0: Extended Lc and Le fields not supported b7=1: Extended Lc and Le fields supported b5, b4=00: no logical channel supported b5, b4=10: channel number assignment by the card Maximum number of channels supported: 4
13	Status indicator tag	‘8x’	Tag for next byte, x is either '2' or '3'
14	Status indicator	[LCS ||] ‘9000’	Life Cycle State (optional) followed by status words SW1-SW2

[a] DO may be present in EF.ATR/INFO for compatible tag

The list and the order of the historical bytes are compulsory unless further items complete these historical bytes according to the smart card manufacturer’s policy (e.g. reference and version of the application).

5.3.3 EF.ATR/INFO

At least one of the options ATR/ATS or EF.ATR/INFO shall be supported.

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

For data objects stored in the EF.ATR/INFO the BER-TLV format is mandatory. All data objects given in Table 2 are mandatory to be contained in EF.ATR/INFO except if they are conditional or not applicable.

In order to identify the compatible tag allocation scheme and the authority responsible for the scheme, the interindustry template referenced by tag '78' is used by the present specification. The allocation authority shall be identified as CEN by an OID with the following root:

ISO (1) identified-organisation (3) CEN (162)

The specification number to be defined according to CEN conventions shall be added to this root to figure the full OID. The corresponding BER-TLV encoded OID shall be nested in the data object '06'.

The DO referenced by tag '78' may be hosted in EF.ATR while the historical byte denoting the Card Service Data shall has bit5 set to one to indicate that a DO is available in EF.ATR.

Alternatively, the D.O. ‘78’ can be hosted by an ADF whereby denoting that the tag allocation scheme applies to data objects within this ADF and not to the whole card.