SLOVENSKI STANDARD
SIST-TS CEN/TS 15480-3:2011

01-februar-2011

Sistemi z identifikacijskimi karticami - Kartica evropskih državljanov - 3. del: Medobratovalnost kartice evropskih državljanov z uporabo aplikacijskega vmesnika

Identification card systems - European Citizen Card - Part 3: European Citizen Card Interoperability using an application interface

Identifikationskartensysteme - Europäische Bürgerkarte - Teil 3: Anwendungsschnittstelle für die Interoperabilität von Europäischen

Systèmes d'Identification par Carte - Carte Européenne de Citoyen - Partie 3: Interoperabilité de la Carte européenne de Citoyen par interface applicative

Ta slovenski standard je istoveten z: **CEN/TS 15480-3:2010**

ICS:

35.240.15	Identifikacijske kartice in sorodne naprave	Identification cards and related devices

SIST-TS CEN/TS 15480-3:2011 **en**

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN/TS 15480-3

December 2010

ICS 35.240.15

English Version

Identification card systems - European Citizen Card - Part 3: European Citizen Card Interoperability using an application interface

Systèmes d'Identification par Carte - Carte Européenne de Citoyen - Partie 3: Interoperabilité de la Carte européenne de Citoyen par interface applicative

Identifikationskartensysteme - Europäische Bürgerkarte - Teil 3: Anwendungsschnittstelle für die Interoperabilität von Europäischen Bürgerkarten

This Technical Specification (CEN/TS) was approved by CEN on 12 July 2010 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 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 15480-3:2010: E

Contents

Page

Foreword

This document (CEN/TS 15480-3:2010) 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.

According to the CEN/CENELEC Internal Regulations, the national standards organizations 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 and the United Kingdom.

1 Scope

ECC part 3 will provide an Interoperability Model, which will enable an eService compliant with technical requirements, to interoperate with different implementations of the European Citizen Card.

This Interoperability model will be developed as follows:

— starting from the ECC part 2, part 3 of the ECC series will provide additional technical specifications for a middleware architecture based on ISO/IEC 24727. This middleware will provide an API to an eService as per ISO/IEC 24727-3;

— a set of additional API provide the middleware stack with means to facilitate ECC services;

— a standard mechanism for the validation of the e-ID credential stored in the ECC and retrieved by the service.

In order to support the ECC services over an ISO/IEC 24727 middelware configuration, this part of the standard specifies the following:

— a set of mandatory requests to be supported by the middleware implementation based on ISO/IEC 24727;

— data set content for interoperability to be personalized in the ECC;

— two middleware architecture solutions: one based on a stack of combined ISO/IEC 24727 configurations and the other based on Web Service configuration;

— a Global Profile featuring the guidelines for card-applications to fit in ISO/IEC 24727 framework.

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.

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

ISO/IEC 7816-3:2008, *Identification cards — Integrated circuit cards — Part 3: Cards with contacts — Electrical interface and transmission protocols*

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

ISO/IEC 7816-8:2004, *Identification cards — Integrated circuit cards — Part 8: Commands for security operations*

ISO/IEC 7816-9, *Identification cards — Integrated circuit cards — Part 9: Commands for card management*

ISO/IEC 7816-15:2004, *Identification cards — Integrated circuit cards with contacts — Part 15: Cryptographic information application*

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

ISO/IEC 9796-2:2002, *Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms*

ISO/IEC 24727-1:2007, *Identification cards — Integrated circuit card programming interfaces — Part 1: Architecture*

ISO/IEC 24727-2:2008 *Identification Cards — Integrated circuit card programming interfaces — Part 2: Generic card interface*

ISO/IEC 24727-3:2008 *Identification Cards — Integrated circuit card programming interfaces — Part 3: Application Interface*

ISO/IEC 24727-4:2008, *Identification cards — Integrated circuit card programming interface — Part 4: Application programming interface (API) Administration*

3 Terms and definitions

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

3.1
descriptive elements
the Application Capability Descriptor (ACD) and the Card Capability Descriptor (CCD) comprehend information nested in data objects and intended for the discovery mechanism. These descriptive elements are encapsulated along with procedural elements in the ACD and CCD. EF.DIR is part of the descriptive elements

3.2
procedural elements
translation code to process any request at the Generic Card Interface (GCI) and every relevant card response. The translation has one entry point, theTranslationCode() function as per ISO/IEC 24727-2

3.3
middleware
set of abstraction layers that serves as the intermediate between a client-application and an application resident in the ECC. The actual pieces of software running behind these abstraction layers are implementation-specific and out of the scope of this document

3.4
service
an eService is an application based locally on the client PC or based somewhere in the internet (e.g. government eService, eBuisness eService…) which offers in combination with the ECC smart card the execution of a task

4 Symbols and abbreviations

4.1 Abbreviations

ADF	Application Dedicated File
AID	Application Identifier
AJAX	Asynchronous JavaScript and XML
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
CAPICOM	Cryptographic API COM Object (http://msdn.microsoft.com)
CAR	Certification Authority Reference
CBC	Cipher Block Chaining
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
CryptoAPI	Cryptographic Application Programming Interface (http://msdn.microsoft.com)
CSP	Crytographic Service Provider
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
GCAL	Generic Card Access Layer
HT	Hash Template
ICC	Integrated Circuit Card
DID	Differential Identity acc. ISO/IEC 24727-3
IFD	Interface Device
IFDH	Interface Device Handler
JSON	Java Script Object Notation (http://www.json.org)
KAT	Control reference template for key agreement
LSB	Least Significant Byte
MAC	Message Authentication Code
MF	Master File
M.U.S.C.L.E	Movement for the Use of Smart Card in Linux Environment
MSE	Manage Security Environment
OID	Object Identifier
PAN	Primary Account Number
PIN	Personal Identification Number
PUK	unblocking password
PK – DH	Public key – Diffie Hellman (asymmetric key base algorithm)
PSO	Perform Security Operation
RFU	Reserved for Future Use
RSA	Rivest Shamir Adleman
SAL	Service Access Layer
SDO	Security Data Object
SCB	Security Condition Byte
SE	Security Environment
SEID	Security Environment IDentifier byte

SM	Secure Messaging
SSD	Security Service Descriptor
TLV	Tag Length Value
UQB	Usage Qualifier Byte

5 ECC fitting in ISO/IEC 24727 model

5.1 ISO/IEC 24727 main features

This standardization initiative (ISO/JTC1/SC17 WG4/TF9) aims to design a new framework for interoperability based on a discovery mechanism of which the following paradigm:

The low level implementation features of the smart card, including proprietary specific features and characteristics based on ISO standards (i.e. ISO/IEC 7816-4) are hidden to the client-application through a high-level description provided to the terminal and processed by the middleware stack.

The middleware stack is defined by abstraction layers ensuring the interoperability. These layers are sustained by applicative components of which the implementation is up to the integrator and may vary according to the environment. For instance, the use of CAPICOM, CryptoAPI, CSP, proprietary API or DLL, ActiveX objects, Applets, PKCS#11 interface, JCE, M.U.S.C.L.E PC/SC emulation on Linux environment etc., are all possible solutions upon which the ISO/IEC 24727abstraction layers may run.

The middleware abstraction layers are of two kinds:

— the Service Access Layer (SAL) is in charge of interpreting the requests addressed by the client-application to the card via a high-level API (the SAL-API). The SAL translates the requests in terms of sequences of APDU that are sent out to the underlying abstraction layer (the GCAL). This translation is performed according to the rules defined by a set of interoperability data reflecting the rules governing the card-applications. The SAL shall generate on the fly these interoperability data out of the ISO/IEC 7816-15 information available in the card. This ISO/IEC 7816-15 information is either provided within the CardApplicationServiceDescription data, or within the DF.CIA files, or both. Upon request from the eService, the SAL may surface the interoperability data to the eService.The SAL is specified in ISO/IEC 24727-3;

— the Generic Card Access Layer (GCAL) is in charge of translating the APDU handed on by the SAL in terms of APDU understandable to the smart card. This translation is applied according to the rules defined in the ACD (Application Capabilities Descriptor) and/or in the CCD (Card Capabilities Descriptor) templates. These templates are read out of the card by the GCAL. The GCAL performs a bootstrap mechanism upon card detection in order to retrieve the ACD and CCD containers from the card. The bootstrap operation is the first step of the discovery mechanism. The GCAL functionality is specified in ISO/IEC 24727-2.

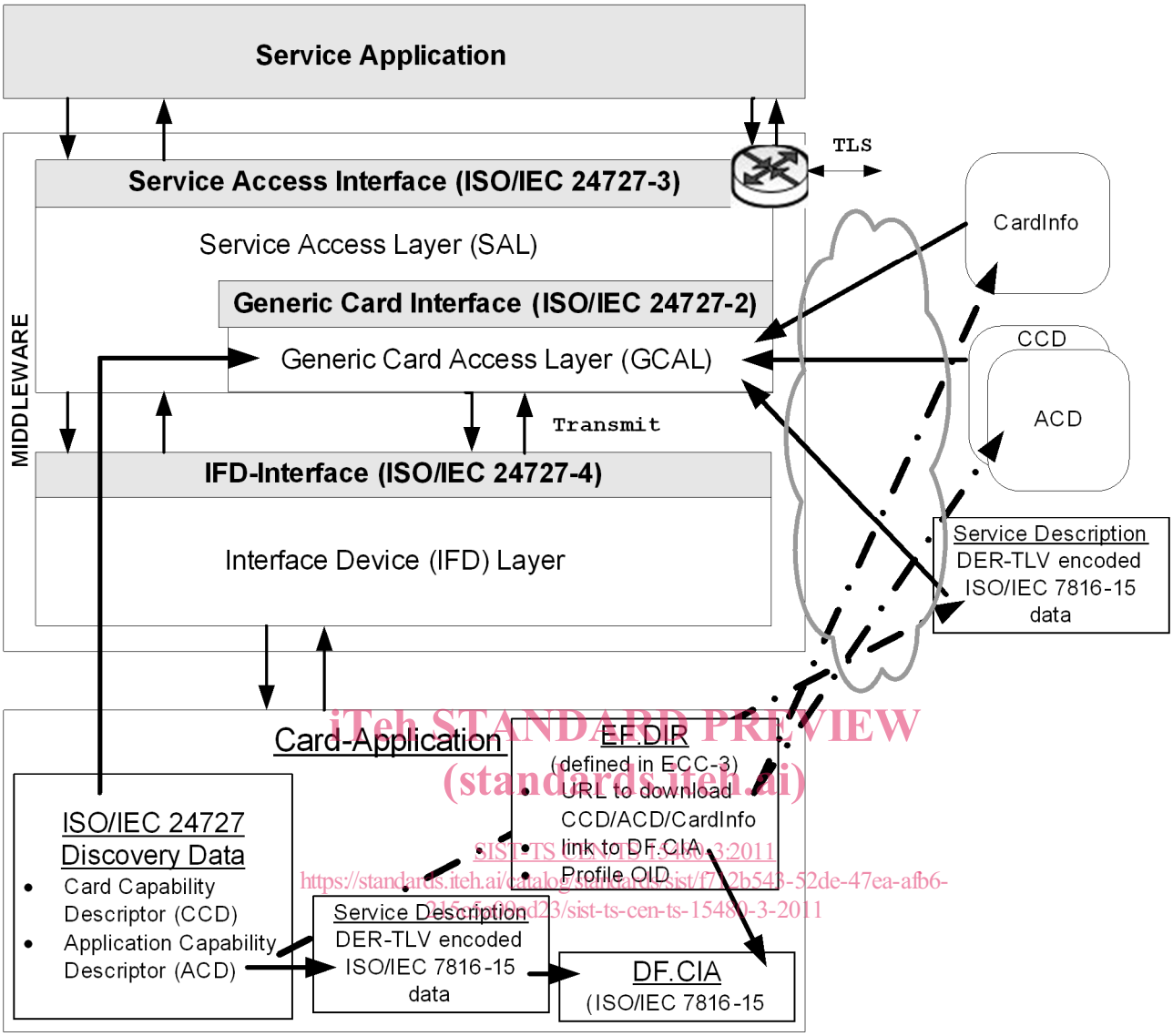

Figure 1 — CEN/TS 15480 compliant smart card in ISO/IEC 24727 framework

The smart card hosts a set of interoperability data that are DER-TLV encoded according to an ASN.1 definition. This ASN.1 specification provided in ISO/IEC 24727-2 describes all the information items required by a terminal to access the services offered by the card (resources, actions) and to allow as well the end-user to access services running on terminal side. This ASN.1 specification is built upon the computational model specified in ISO/IEC 24727-3. Therefore, the ASN.1 definition encompasses the descriptors of the services hosted on-card per application, the card application list, the access control rules applying to each on-card action or resource, and the description of each modular authentication item (called Differential-Identity or DID). This latter item (Figure 2 — Differential-Identity structure according to ISO/IEC 24727-3) is the modular descriptor of each authentication procedure. DID is comprised of five fields among which an optional element, the dIDQualifier, that conveys further information to clear ambiguities whenever required by cryptographic requests.

Element 1	Element 2	Element 3	Element 4	Element 5
DIDName Mandatory	Authentication Protocol Mandatory	Marker Mandatory	Scope (Global or Local; implicit)	dIDQualifier Optional

Figure 2 — Differential-Identity structure acc. ISO/IEC 24727-3

The relationship between the elements constituting a DID is such as a Marker applied in a given Scope feeds the algorithm of a given Authentication Protocol that is applied to authenticate a given named DID.

The rules controlling the access to a card resource or authorizing a card action are expressed has a Boolean combination of Differential-Identities. If the Boolean expression evaluates to "TRUE", the requested card resources are made available or the card action is executed, otherwise the request is rejected.

The DifferentialIdentityQualifier may serve to convey to the SAL the OID related to a cryptographic operation or authentication protocol. The DIDQualifier type depends on the Authentication Protocol to which it applies. Details of DIDQualifiers are given in ISO/IEC 24727-3:2008, Annex A.

5.2 General security issues – Applicable 24727-4 Stack Configurations for the ECC environment

The abstraction layers defined by ISO/IEC 24727 are intended to hide seamlessly the implementation differences that may occur between smart cards from different vendors even when their respective implementation is based on the same standard or specification (i.e. CEN/TS 15480-2)

A high level description (according to ISO/IEC 24727) of the security rules governing the services hosted by the card allows and extension of the information provided by ISO/IEC 7816-15 implementation, ensuring thereby a more comprehensive interoperability protocol based on ISO/IEC 7816-15.

By personalizing the necessary data sets for interoperability as per ISO/IEC 24727-2 and ISO/IEC 24727-3, a European Citizen Card can fit in the ISO/IEC 24727 framework with the following limitations:

— the GCAL being assumed to translate APDU handed on by the SAL, these command APDU can not be secured (integrity, confidentiality) otherwise any change in the command header according to the ACD procedural elements will cause a rejection of the command by the smart card. Therefore, if the translation function of the GCAL is performed, end-to-end Secure Messaging cannot be applied between the client-application and the card-application in the ISO/IEC 24727 framework. With this respect, the European Citizen Card needs to discard the GCAL translation function unless for use cases where no Secure Messaging is envisioned;

— the Loyal-stack configuration (Figure 3 — ISO/IEC 24727-4 excerpt: Loyal-Stack configuration), the Remote-ICC-stack configuration (Figure 4 — ISO/IEC 24727-4 excerpt: Remote-ICC-Stack configuration), and the Remote-Loyal-Stack configuration (Figure 5 — ISO/IEC 24727-4 excerpt: Remote-Loyal-Stack configuration) are considered in the present document. A generic depiction of ISO 24727 middleware stack lying over different platforms is represented on Figure 6 — ISO/IEC 24727-4 excerpt: Generic elements of ISO/IEC 24727 MW stack);