SLOVENSKI STANDARD
SIST-TS CEN/TS 15480-3:2014

01-julij-2014

Nadomešča:

SIST-TS CEN/TS 15480-3:2011

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 Bürgerkarten

Systèmes de carte d’identification - Carte Européenne du Citoyen - Partie 3 : Interopérabilité de la Carte européenne du Citoyen utilisant une interface applicative

Ta slovenski standard je istoveten z: **CEN/TS 15480-3:2014**

ICS:

35.240.15	Identifikacijske kartice in sorodne naprave	Identification cards and related devices

SIST-TS CEN/TS 15480-3:2014 **en,fr,de**

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN/TS 15480-3

April 2014

ICS 35.240.15

Supersedes CEN/TS 15480-3:2010

English Version

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

Systèmes de carte d'identification - Carte Européenne du Citoyen - Partie 3 : Interopérabilité de la Carte européenne du Citoyen utilisant une interface applicative

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

This Technical Specification (CEN/TS) was approved by CEN on 14 October 2013 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, Former Yugoslav Republic of Macedonia, 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

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. CEN/TS 15480-3:2014 E

Contents

Page

Foreword

This document (CEN/TS 15480-3:2014) 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 15480-3:2010.

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

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

— *Part 2: Logical data structures and security services*;

— *Part 3: European Citizen Card Interoperability using an application interface* (the present document);

— *Part 4: Recommendations for European Citizen Card issuance, operation and use*;

— *Part 5: General Introduction*.

The following technical changes have been made in this new edition of CEN/TS 15480-3:

— addition of mention of SAL Lite component, abstraction of GCI and GCAL through Registry processed at SAL level, decision tree update, scope update, etc (5.3.5.3);

— removal of all subclauses under 6.6.3 (Data structures mapping) that were already incorporated in ISO/IEC 24727-4;

— removal of Annex J dedicated to ECC-3 API (handling ISO/IEC 7816-15 objects) considered not appropriate in ECC-3 because implementation-specific and not fundamental to interoperability;

— removal of XML Binding details for SAL API from Clause 10 and Annex G (removal of Annex G); it was incorporated in ISO/IEC 24727-3:2008/DAmd 1, Annex F;

— maintainance of the annex investigating SAL post-issuance personalisation;

— removal of Annex H describing XML binding for Authentication protocols since these protocols are now part of ISO/IEC 24727-3:2008/DAmd 1, i.e. EACv2 protocol binding doesn’t need to be reflected in ECC-3 since it is incorporated in ISO/IEC 24727-3:2008, Annex E;

— removal of Annex D “example of CIA implementation for Card –Application Service description” since it is updated and incorporated in ISO/IEC 24727-4:2008/DAmd 1;

— removal of XML-based CardInfo Types (XML Registry) since it is incorporated in ISO/IEC 24727-3:2008/DAmd 1, Annex D, Clause D.3;

— IFD-API shows enhancements in comparison with ISO/IEC 24727 (e.g. SlotCapabilityType with support of transmission protocol descriptor, Transmit command with support of batch APDU, SignalEvent error coding with additional error code), therefore IFD API Annex B are removed from ECC-3 and the clauses describing enhancements are reflected in ECC-3, Annex D amongst the differences with ISO/IEC 24727;

- addition of Annex D, Additional features versus ISO/IEC 24727 (all parts), to incorporate the description of IFD API extensions in terms of API definition and binding;

- removal of 6.2.1.1, Definition for CardInfoRepository.XSD, and 6.2.1.2, Definition for CardInfoRepository.WSDL, since these binding descriptions are now part of ISO/IEC 24727-4:2008/DAmd, 1;

- addition of a new Clause 11 dedicated to Authenticate API: the Authenticate() call makes the service layer module transparent to the Service Provider, it occurs above SAL layer;

- provision of an introductory text describing the layout where Authenticate API fits;

- IFD API C-Language Binding remains in ECC-3 till its endorsement in ISO/IEC 24727 if deemed useful;

- maintainance of ExecuteSAL API in ECC-3 (both C-language binding and java binding);

- incorporation under Annex G of “Application Discovery Profile” for the purposes of integration in ISO/IEC 24727 framework.

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, Former Yugoslav Republic of Macedonia, 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 provides 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 provides additional technical specifications for a middleware architecture based on ISO/IEC 24727 (all parts); this middleware will provide an API to an eService as per ISO/IEC 24727-3.

— a set of additional API provides the middleware stack with means to facilitate ECC services.

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

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 (all parts).

— data set content for interoperability to be personalised in the ECC.

— three middleware architecture solutions: one based on a stack of combined ISO/IEC 24727 configurations and the other based on Web Service configuration whereas the third one is relying on a SAL Lite component.

— an Application DiscoveryProfile featuring the guidelines for card-applications to fit in ISO/IEC 24727 framework.

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.

CEN/TS 15480-2:2012, *Identification card systems — European Citizen Card — Part 2: Logical data structures and security services*

CEN/TS 15480-4, *Identification card systems — European Citizen Card — Part 4: Recommendations for European Citizen Card issuance, operation and use*

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

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

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

ISO/IEC 24727-2:2008 [1], *Identification cards — Integrated circuit card programming interfaces — Part 2: Generic card interface*

ISO/IEC 24727-3:2008 [2], *Identification cards — Integrated circuit card programming interfaces — Part 3: Application interface*

ISO/IEC 24727-4:2008 [3], *Identification cards — Integrated circuit card programming interfaces — Part 4: Application programming interface (API) administration*

ISO/IEC 24727-5, *Identification cards — Integrated circuit card programming interfaces — Part 5: Testing procedures*

ISO/IEC 24727-6, *Identification cards — Integrated circuit card programming interfaces — Part 6: Registration authority procedures for the authentication protocols for interoperability*

3 Terms and definitions

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

3.1
descriptive elements
information nested in data objects and intended for the discovery mechanism and encapsulated along with procedural elements in the ACD and CCD

3.2
procedural elements
translation code to process any request at the Generic Card Interface (GCI) and every relevant card response

Note 1 to entry: The translation has one entry point, theTranslationCode() function as per ISO/IEC 24727-2.

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

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

4 Symbols and abbreviations

ADF	Application Dedicated File
AID	Application Identifier
AJAX	Asynchronous JavaScript and XML
AMB	Access Mode Byte
AT	Authentication Template

[1] This document is currently impacted by the draft amendment ISO/IEC 24727-2:2008/DAmd 1.

[2] This document is currently impacted by the draft amendment ISO/IEC 24727-3:2008/DAmd 1.

[3] This document is currently impacted by the draft amendment ISO/IEC 24727-4:2008/DAmd 1.

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 Authorization
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 according to 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
SAL Lite	Service Access Layer Lite
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 24727 abstraction 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 Part 3 of the ISO/IEC 24727 series.

— 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 Capability Descriptor) and/or in the CCD (Card Capability 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 Part 2 of the ISO/IEC 24727 series.

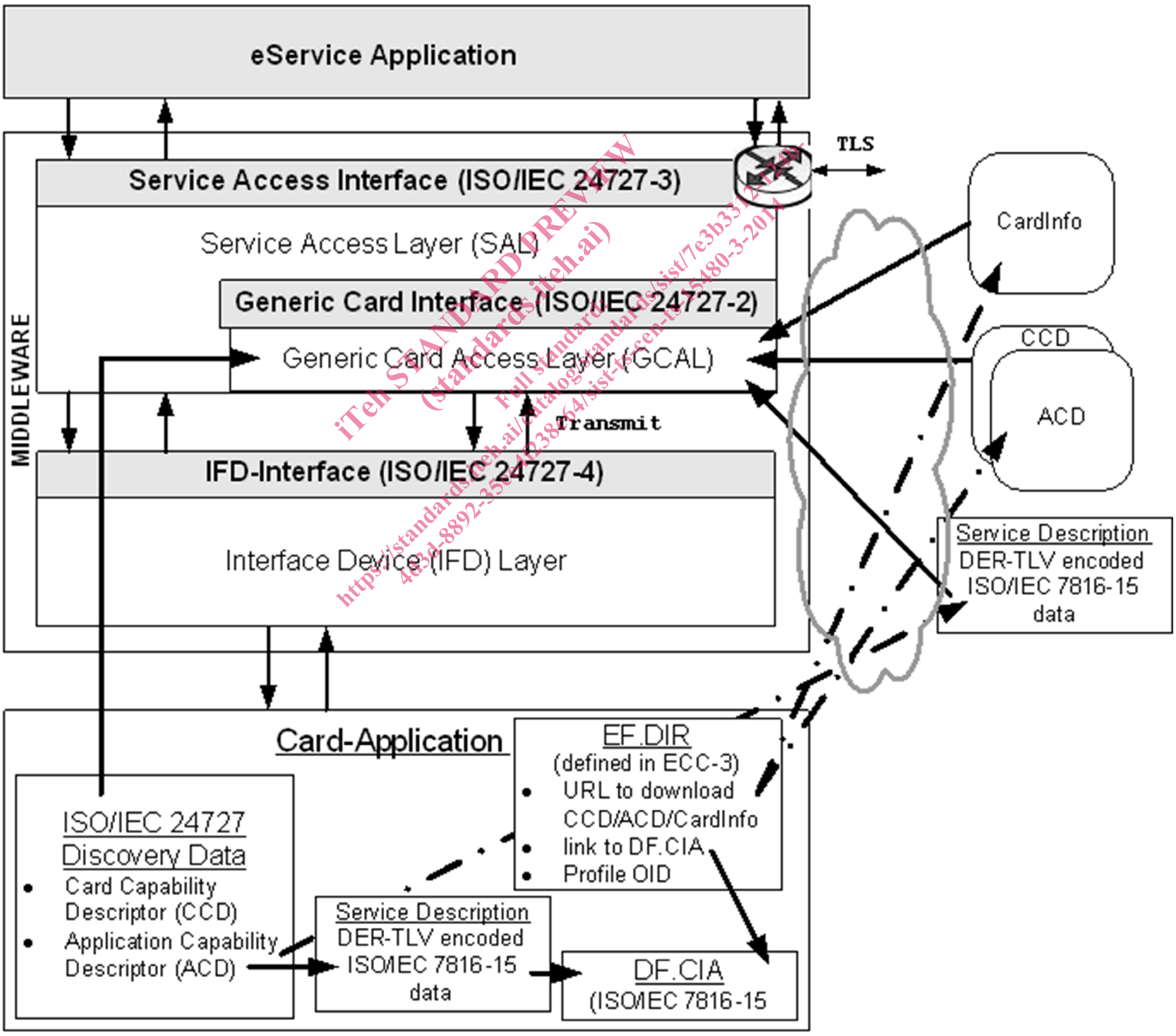

Figure 1 — CEN/TS 15480 compliant smart card in ISO/IEC 24727 framework

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