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 6
1 Scope 7
2 Normative references 7
3 Terms and definitions 8
4 Symbols and abbreviations 8
4.1 Abbreviations 8
5 ECC fitting in ISO/IEC 24727 model 11
5.1 ISO/IEC 24727 main features 11
5.2 General security issues – Applicable 24727-4 Stack Configurations for the ECC environment 13
5.3 ECC-3 Middleware Architecture 16
5.3.1 Service Access Layer (SAL) 17
5.3.2 Generic Card Access Layer (GCAL) 17
5.3.3 Interface Device Layer and API (IFD API) 17
5.3.4 ECC-3 Stack Distribution and Connection Handling 17
5.3.5 A Web Service based architecture for ECC-3 framework 21
5.3.6 XML-based SAL interface 26
5.3.7 Smart card profile fitting with ECC-3 stack 26
6 Card Discovery Mechanisms 27
6.1 Discovery decision tree 28
6.2 Migration path towards ECC and provision for legacy cards 29
6.2.1 Interoperable access to the Repository 30
6.3 Set of data for interoperability 32
6.4 Application and Card Capability Descriptors 32
6.5 ISO/IEC 7816-15 implementation 34
6.5.1 Profile designation within EF.DIR 35
6.5.2 ISO/IEC 24727-3 data structures mapping 35
6.5.3 SAL-API Action mapping onto ISO/IEC 7816-15 attributes 51
6.5.4 ISO/IEC 24727-3 data structures storage onto the card 53
6.5.5 General discovery mechanism 55
6.6 Other data descriptor 57
7 Authentication protocols 57
7.1 Authentication Mechanisms based on ISO/IEC 24727 SAL-API 57
7.2 Asymmetric internal authentication 58
7.3 Asymmetric external authentication 58
7.4 Symmetric internal authentication 58
7.5 Symmetric external authentication 59
7.6 Mutual authentication with key establishment 59
7.7 Device authentication with non traceability 59
7.8 Key transport protocol based on RSA 59
7.9 Terminal Authentication 60
8 IFD-API Web Service Binding 60
8.1 Specification of ISOCommon.XSD 60
8.2 Specification of ISOIFD.XSD 61
8.3 Specification of CENIFD.WSDL 74
8.4 Specification of CENIFDCallback.XSD 83
8.5 Definition of CENCallback.WSDL 84

9 Card-Info Structure 85
9.1 Introduction 85
9.2 Overview 86
9.3 CardType 87
9.4 CardIdentification 88
9.5 CardCapabilities 94
9.6 ApplicationCapabilities 103
9.7 Signature 109
9.8 Complete XML-Schema Definition 109

10 XML-based Service Access Layer Interface 112
10.1 XML-Schema definitions for Service Access Layer functions 112
10.2 WSDL definitions for Service Access Layer functions 137

Annex A (informative) **Interface Device Layer Architecture and Management 161**
A.1 Scope 161
A.2 IFD-Layer Architecture 161
A.3 Resource Manager 162
A.3.1 IFD-Handlers 162
A.3.2 Card transactions 162
A.3.3 Application threads 162
A.4 Administrative functions 162
A.4.1 IFD-Handler related functions 162
A.4.2 Interface Device related functions 163
A.5 IFD-Handler-API 163

Annex B (informative) **Interface Device API 164**
B.1 Card terminal related functions 164
B.1.1 EstablishContext 164
B.1.2 ReleaseContext 165
B.1.3 ListIFDs 165
B.1.4 GetIFDCapabilities 166
B.1.5 GetStatus 168
B.1.6 Wait 170
B.1.7 Cancel 171
B.1.8 ControlIFD 172
B.2 Card related functions 172
B.2.1 Connect 173
B.2.2 Disconnect 174
B.2.3 BeginTransaction 174
B.2.4 EndTransaction 175
B.2.5 Transmit 175
B.3 User related functions 176
B.3.1 VerifyUser 177
B.3.2 ModifyVerificationData 179
B.3.3 Output 181

Annex C (informative) **IFD-API – C Language Binding 183**

Annex D (informative) **Examples of Cryptographic Information Application for Card-Application Service Description 189**
D.1 Fetching a certificate for internal asymmetric authentication 189
D.2 Creating a new service 190
D.2.1 Features of eVoting Service 190

Annex E (informative) **SAL-API Post-issuance personalization requests 204**
E.1 Post-issuance personalization requests 204
E.2 Canonical protocol 204
E.2.1 DataSetCreate 205
E.2.2 DSICreate 213
E.2.3 DIDCreate 214
E.2.4 DIDUpdate 216

E.2.5 CardApplicationServiceCreate 216

Annex F (informative) Additional features versus ISO/IEC 24727 219
F.1 Discovery Mechanism 219
F.2 General Procedures (SAL) 220
F.3 Architecture 221
F.4 eURI support (through ControlIFD() call) 222
F.5 Differences between IFD-API in ISO/IEC 24727-4 and ECC-3 222
F.5.1 More generale SlotCapabilityType 222
F.5.2 Transmit with support for batch processing 222
F.5.3 Additional error code for Signalevent 222
F.6 Miscellaneous corrections 222

Annex G (informative) C-Language Binding for ExecuteSAL function 223

Annex H (informative) Java-Language Binding for ExecuteSAL function 224

Annex I (informative) XML-Binding for Authentication Protocols 225
I.1 PIN Compare 225
I.1.1 Marker 225
I.1.2 DIDCreate 232
I.2 Mutual authentication 234
I.2.1 Marker 235
I.3 RSA Authentication 240
I.3.1 Marker 241
I.3.2 DIDCreate 244
I.3.3 DIDUpdate 244
I.3.4 DIDGet 244
I.3.5 CardApplicationStartSession 244
I.3.6 DIDAuthenticate 245
I.4 Generic cryptography 248
I.4.1 Marker 249
I.4.2 DIDCreate 254
I.4.3 DIDUpdate 254
I.4.4 DIDGet 254
I.4.5 Encipher 254
I.4.6 Decipher 254
I.4.7 GetRandom 254
I.4.8 Hash 254
I.4.9 Sign 254
I.4.10 VerifySignature 254
I.4.11 VerifyCertificate 254
I.4.12 DIDAuthenticate 255

Annex J (informative) API for ISO/IEC 7816-15 data structures handling 257
J.1 C-language Binding for the ECC3-API 259
J.1.1 ECC3RESULT 259
J.1.2 ECC3CONTEXT 259
J.1.3 ECC3INFO 259
J.1.4 ECC3VERSION 260
J.1.5 CioChoice 260
J.1.6 CommonObjectFlags 260
J.1.7 SecurityEnvironmentInfo 260
J.1.8 AlgorithmInfo 261
J.1.9 PasswordType 261
J.1.10 Validity 261
J.1.11 ObjectValueType 261
J.1.12 FileType 262
J.1.13 FileState 262
J.1.14 IdType 262
J.1.15 AccessModes 263
J.1.16 Operations 263

J.1.17 ContextTag 263
J.1.18 SecurityConditionType 264
J.1.19 DataSetNameType 264
J.1.20 DSINameType 264
J.2 Interface functions 265
J.2.1 General Purposes Functions 265
J.2.2 Reader and Card management Functions 265
J.3 Objects 266
J.3.1 Basic objects 266
J.3.2 File Objects 275
J.3.3 Data Objects 283
J.4 Macros 292
J.4.1 _HB: HexaBlob convertions 292
J.4.2 AsString 293
J.5 Example of use (C++ Language) 293

Annex K (informative) **Global Profile 4: card requirements to access/offer services in ISO/IEC 24727 framework** 295
K.1 Global Profile 4: Card requirements 295
K.1.1 OID 295
K.1.2 General 295
K.1.3 interfaces / transport protocols 295
K.1.4 Data elements and data structures 296
K.1.5 Command set 298
K.1.6 Data structure of Card Applications 299

Bibliography 300

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