PD CEN/TS 15480-3:2014

BSI Standards Publication

Identification card systems — European Citizen Card

Part 3: European Citizen Card Interoperability using an application interface

bsi.

...making excellence a habit.™

National foreword

This Published Document is the UK implementation of CEN/TS 15480-3:2014. It supersedes DD CEN/TS 15480-3:2010 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/17, Cards and personal identification.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2014

ISBN 978 0 580 82884 3
ICS 35.240.15

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 April 2014.

Amendments/corrigenda issued since publication

Date	Text affected

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 **5**

1 Scope **7**

2 Normative references **7**

3 Terms and definitions **8**

4 Symbols and abbreviations **8**

5 ECC fitting in ISO/IEC 24727 model **10**
5.1 ISO/IEC 24727 main features **10**
5.2 General security issues – Applicable ISO/IEC 24727-4 Stack Configurations for the ECC environment **12**
5.3 ECC-3 Middleware Architecture **16**
5.3.1 General **16**
5.3.2 Service Access Layer (SAL) **17**
5.3.3 Generic Card Access Layer (GCAL) **17**
5.3.4 Interface Device Layer and API (IFD API) **17**
5.3.5 ECC-3 Stack Distribution and Connection Handling **17**
5.3.6 Multi-stack composed configuration **20**
5.3.7 A Web Service based architecture for ECC-3 framework **22**
5.3.8 XML-based SAL interface **27**

6 Card Discovery Mechanisms **28**
6.1 General **28**
6.2 Discovery decision tree **29**
6.3 Migration path towards ECC and provision for legacy cards **29**
6.3.1 General **29**
6.3.2 Interoperable access to the Repository **30**
6.4 Set of data for interoperability **30**
6.5 Application and Card Capability Descriptors **31**
6.6 ISO/IEC 7816-15 implementation **34**
6.6.1 General **34**
6.6.2 Profile designation within EF.DIR **34**
6.6.3 ISO/IEC 24727-3 data structures mapping **35**
6.6.4 ISO/IEC 24727-3 data structures storage onto the card **35**
6.6.5 General discovery mechanism **37**
6.7 Other data descriptor **39**

7 Authentication protocols **39**
7.1 General **39**
7.2 Authentication Mechanisms based on ISO/IEC 24727 SAL-API **39**
7.3 Asymmetric internal authentication **40**
7.4 Asymmetric external authentication **40**
7.5 Symmetric internal authentication **41**
7.6 Symmetric external authentication **41**
7.7 Mutual authentication with key establishment **41**
7.8 Device authentication with non traceability **41**
7.9 Key transport protocol based on RSA **41**
7.10 Terminal Authentication **42**

8 IFD-API Web Service Binding **42**

9 Card-Info Structure — Introduction **42**

10 XML-based Service Access Layer Interface 43

11 Federative Framework-wise Authenticate API 43
11.1 General 43
11.2 Authenticate method 44
11.3 Web Service Binding for Authenticate API 47
11.3.1 General 47
11.3.2 Authenticate.XSD definition 47
11.3.3 Authenticate.WSDL definition 48

Annex A (informative) **Interface Device Layer Architecture and Management 51**
A.1 Scope 51
A.2 IFD-Layer Architecture 51
A.3 Resource Manager 52
A.3.1 General 52
A.3.2 IFD-Handlers 52
A.3.3 Card transactions 52
A.3.4 Application threads 52
A.4 Administrative functions 52
A.4.1 IFD-Handler related functions 52
A.4.2 Interface Device related functions 53

Annex B (informative) **IFD-API – C Language Binding 54**

Annex C (informative) **SAL-API Post-issuance personalisation requests 60**
C.1 General 60
C.2 Post-issuance personalisation requests 60
C.3 Canonical protocol 60
C.3.1 General 60
C.3.2 DataSetCreate 61
C.3.3 DSICreate 68
C.3.4 DIDCreate 70
C.3.5 DIDUpdate 71
C.3.6 CardApplicationServiceCreate 72
C.4 General recommendation and conclusion 74

Annex D (informative) **Additional features versus ISO/IEC 24727 (all parts) 75**
D.1 General 75
D.2 Discovery Mechanism 75
D.3 General Procedures (SAL) 75
D.4 Architecture 77
D.5 Differences between IFD-API in ISO/IEC 24727-4 and ECC-3 77
D.5.1 More generale SlotCapabilityType 77
D.5.2 Transmit with support for batch processing 80
D.5.3 Additional error code for SignalEvent 82

Annex E (informative) **C-Language Binding for ExecuteSAL function 83**

Annex F (informative) **Java-Language Binding for ExecuteSAL function 84**

Annex G (informative) **Application Discovery Profile: card requirements to access/offer services in ISO/IEC 24727 framework 85**
G.1 General 85
G.2 OID 85
G.3 General 85
G.4 interfaces / transport protocols 85
G.5 Data elements and data structures 86
G.6 Command set 88
G.7 Data structure of Card Applications 89
G.7.1 General 89
G.7.2 DF/ADF content 89

G.7.3 EF DCOD content 89
G.7.4 EF AOD content 90
G.7.5 EF SKD content 90
G.7.6 Ef PrKD content 90

Bibliography 91

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*