SLOVENSKI STANDARD
SIST-TS CEN/TS 15480-5:2013

01-junij-2013

Sistemi z identifikacijskimi karticami - Kartica evropskih državljanov - 5. del: Splošna predstavitev

Identification card systems - European Citizen Card - Part 5: General Introduction

Identifikationskartensysteme - Europäische Bürgerkarte - Teil 5: Allgemeine Einführung (ECC-5)

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Systèmes de cartes d'identification - Carte Européene du Citoyen - Partie 5 : Introduction générale (ECC-5)

Ta slovenski standard je istoveten z: **CEN/TS 15480-5:2013**

ICS:

35.240.15	Identifikacijske kartice in sorodne naprave	Identification cards and related devices

SIST-TS CEN/TS 15480-5:2013 **en,fr,de**

2003-01.Slovenski inštitut za standardizacijo. Razmnoževanje celote ali delov tega standarda ni dovoljeno.

iTeh STANDARD PREVIEW

(standards.iteh.ai)

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN/TS 15480-5

April 2013

ICS 35.240.15

English Version

Identification card systems - European Citizen Card - Part 5: General Introduction

Systèmes de cartes d'identification - Carte Européene du Citoyen - Partie 5 : Introduction générale (ECC-5)

Identifikationskartensysteme - Europäische Bürgerkarte - Teil 5: Allgemeine Einführung (ECC-5)

This Technical Specification (CEN/TS) was approved by CEN on 12 February 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

Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. CEN/TS 15480-5:2013: E

CEN/TS 15480-5:2013 (E)

Contents

Page

Foreword

This document (CEN/TS 15480-5:2013) 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 organisations 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

CEN/TS 15480-5:2013 (E)

Introduction

Within the European Union there will be many integrated circuit cards issued by public bodies and administrations, each of which can house a variety of applications in different combinations. The cardholder can hold several multi-application public service cards and is concerned that:

— He or she knows or can find out which applications are on a card;

— Applications on a card may be read and dealt with by appropriate terminals;

— Security is appropriate for the application being used, while also being fit-for-purpose in protecting the user's data on the card and ensuring privacy to the level required.

Different cards will have different capabilities. This presents application providers and scheme operators with a number of challenges:

— Does the card have the specific minimum level of functionality, capability and security features necessary to house the application to be loaded onto the card?

— Are there other applications on this card that would preclude this application being loaded (including for example, surface printing requirements)?

— What are the features and functions of the card (that are being used) that the terminal will have to support?

This Technical Specification provides mechanisms to resolve the above issues together with a formalised approach that will allow different applications and services to co-exist and interoperate in a single card environment.

This Technical Specification also recognises that there will be legacy systems in evidence as and when the ECC card is being introduced. It provides a mechanism (described in CEN/TS 15480-3) by which legacy systems can operate in an ECC environment until cards may be replaced by European Citizen Cards in batches as the opportunity arises.

1 Scope

1.1 Scope of CEN/TS 15480-5:2013

The scope of this Technical Specification is to provide a general description of the standard together with an introduction to each part of the ECC standard.

Informative Annex A maps the relationship between the various parts of the ECC standard and other ISO/IEC standards relating to the card platform.

1.2 Scope of the ECC standard

The European Citizen Card (ECC) standard addresses the difficulties presented to citizens when attempting to access various public services using a smart card as an access token. The scope of the ECC standard covers card capabilities and structures specified under the following headings:

— Specific definition of minimum features (for example, card surface print structure).

— Definition of optional features that may be required to provide the desired electronic services.

— Specification of discovery mechanisms to allow supported and in-use card capabilities and features to be identified.

— Besides covering the hardware and software of the card, the ECC standard also addresses interfaces to readers and servers through middleware components.

This simple concept can enable ECC cards to adopt a widely different set of personas, even though a common application may be housed on cards used in different environments and in different ways. Generically, we can consider ECC cards as being classed as one of the following groups, even though the same application may be loaded (alongside others) in each environment. These groupings are:

— eID Verification token;

— Inter-European Union travel document;

— Provider of logical access to e-Government or local administration services or to private sector services by housing personal credentials.

In order to support the above, it is noted that there will be certain minimum requirements upon any card conforming to the ECC, specifically, the European Citizen Card will be at a minimum a smart card with Identification, Authentication and electronic Signature (IAS) service capabilities. The ECC may act as a bridge between different application requirements of an integrated circuit card and in so doing act to reduce the number of different European specifications and standards required.

The ECC will be issued under the responsibility of a European National Public Administration in order to provide a token supporting one of the above usage groupings by housing one or more relevant applications. In addition, there is nothing to stop the ECC being used to support private applications and environments which would therefore allow the ECC to be used in a shared public-private application scenario.

It is apparent that the ECC is intended to offer the card issuer/ service provider with a great deal of flexibility in the services that the ECC provides, the authentication mechanisms supported and the local national specific public policy with an special concern to protect the citizen privacy according to the applicable European legislation.

2 Normative references

Not applicable.

3 Terms and definitions

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

3.1
ECC Application Profile
set of ECC mandatory and optional features which is referred to by a unique registered identifier. An Application Profile implements an interoperable ECC service

3.2
ECC Card Profile
profile made up of one or more ECC Application Profiles with their associated electrical interfaces and possibly one or more ECC User Accessibility Profiles. In addition an ECC Card Profile may also include an ECC Durability Profile. An ECC Card Profile is referred to by a unique registered identifier

3.3
ECC Conditional Feature
feature required by an ECC Application Profile

3.4
ECC Durability Profile
profile associated with an ECC, which provides information that relates to the card durability performance

3.5
ECC Layout Profile
optional profile which indicates card body requirements

3.6
ECC Mandatory Feature
card software feature required to claim compliance with the ECC standard

3.7
ECC Optional Feature
card software feature not required to claim compliance with an ECC

3.8
ECC User Accessibility Profile
set of card optional features not identified in any ECC Application Profile supported by the card and which may improve the accessibility to services and/or the usability of the ECC. An ECC User Accessibility Profile is referred to by a unique registered identifier

3.9
ECC Discovery Profile
set of features supported by the card-applications and personalised in different formats depending on card issuer's choice. Once read by the terminal, this profile uncovers card-application services with their related data references and the security rules applying to it. This profile allows ECC fitting in an ISO/IEC 24727 framework

4 Symbols and abbreviations

EF   Elementary File

EF.DIR   Elementary File Directory

ELC   Elliptic Curve cryptography

5 Construction of the ECC standard

The ECC standard is specified in five parts as follows:

1) Part 1: Specifies the physical characteristics and construction of the card including:

   a) card body;

   b) electrical interfaces;

   c) data transport protocols;

   d) authentication elements visible at the card surface;

   e) the specification of an ECC Layout Profile and an ECC Durability Profile;

2) Part 2: Specifies the logical characteristics and security features at the card/system Interface. These include:

   a) the specification of supported services;

   b) the specification of supported data structures as well as the access to them;

   c) the definition of the command set;

   d) the specification of ECC Application Profiles;

3) Part 3: Covers the achievement of interoperability using an application interface. In particular, this part covers how interoperability can be achieved:

   a) to fit in a framework designed based on ISO/IEC 24727;

   b) to provide a means for legacy card support within the ECC framework;

   c) the specification of ECC Application Discovery Profile;

4) Part 4: Looks at operational and policy issues:

   a) recommends card issuance and operational procedures including citizen registration;

   b) makes recommendations for citizen contact and interaction (for example, accessibility, usability, privacy and health and safety issues);

   c) specifies a number of ECC Card Profiles and ECC User Accessibility Profiles;

5) Part 5: This introductory and overview document.

Parts 1 to 4 of the ECC standard are explained in more detail in Clauses 8 to 11.

6 Clarification of key concepts used in the ECC standard

6.1 Interoperability

This standard is about interoperability in access to services. However, interoperability is a wide ranging concept and its use within this standard requires further qualification.

CEN/TS 15480-5:2013 (E)

Interoperability in this context is about integrated circuit cards issued in one environment being able to be used in another, where environments may specify different controlling public administrations, different application environments and different card issuers. This does not, however, imply that all cards are the same, all applications are the same, all terminals are the same and all security controls are the same. Rather, this standard defines an open framework for interoperability:

— at the highest level interoperability will be defined by agreements between different service providers within the same or different public administrations;

— at the lowest level the card must be physically readable in the terminal implying compatibility with ISO/IEC 7816-1, 2, and 3 for contact interface cards or ISO/IEC 14443-1,2 and 3 for contactless interface cards;

— this standard defines the minimum requirements of card level service support required of the ECC. Optional additional support may be required for access to certain services. Only those cards supporting the additional requirements will be able to access those services;

— terminals must support the environment in which they exist. However, by design and service operator agreement, that does not mean that all services can be accessed by all terminals. ISO/IEC 24727 may apply to the terminals and surrounding environment (servers), in which case Part 3 of this standard defines the additional interoperability requirements which may or may not be available in the card.

It will be seen that full any-to-any interoperability is not intended or provided for. However, this standard provides a basis for interoperability within a multiplicity of environments in which different cards with different capabilities will operate, issued by different issuers, representing different public administrations and accessing different services each with its own access requirements. Depending upon the circumstances applying, for example commonality of basic card support, this standard offers a way of migrating to the ECC environment, gradually, one legacy system at a time, while continuing to interoperate.

6.2 Privacy

Privacy principles for card issuance and operation as well as privacy features for ECC along with recommendations and legislation guidance can be found in CEN/TS 15480-4:2012 respectively in 5.1 and Clause 6. References to EU legal acts can be found in CEN/TS 15480-4:2012, Annex C. Privacy-compliant implementation examples are provided in CEN/TS 15480-2:2012 as reference to authentication protocols (see 6.4.4.3 for Device authentication with privacy protection, or 7.8 for Restricted Identification, or 7.10 for modular Enhanced Role Authentication) or as Application Profiles (see E.4 for Profile 3 "eID Application", or E.6 for Profile 5 "eServices Application with Trusted Third Party").

6.3 ECC Profiles

6.3.1   General

The ECC as defined in this standard specifies a minimum set of requirements plus a set of options that may be used in different circumstances as required. ECC Profiles are optional and if used, an example of the set of minimum requirements plus optional facilities that are most likely (or may be mandated) to be used in different usage scenarios. If different card issuers meet the requirement set down in a specific profile,, then interoperability will be guaranteed. One example could be a profile for an ECC to act as a European Travel Document.

Open profiles will be registered and given unique numbers as part of this standard which may be discovered by the card terminal in which the ECC is placed. This enables the terminal quickly to determine whether this ECC supports the service being accessed or provided at this terminal. Private, proprietary profiles may also be defined, however, interoperability will only be guaranteed among terminals recognising and supporting these profiles.

Any national body member of CEN/TC 224 may submit an ECC Profile to CEN/TC 224/WG 15 acting as the Registration Authority for integration in the standard. An ECC may also be issued supporting one or more Proprietary ECC Profiles which shall not be allocated or reuse any registered ECC Profile identifier.

It is perfectly possible for a card to support multiple profiles indicating its multi-application capability where different applications require different profiles each indicating the card support required. It is noted that the actual card services required by different profiles on a card may overlap or even be the same.

6.3.2   Types of profiles defined in the ECC standard

The basic interoperability profile is the ECC Application Profile. If present, it specifies those mandatory and optional features of the ECC required to implement an interoperable ECC service. There may be more than one ECC Application Profile, indicating perhaps overlapping features, each profile indicating the requirements of a different ECC service. ECC Application Profiles may be created, managed and maintained during the life of the ECC. Correspondingly, other ECC Profiles discussed below may also be managed during the life of the ECC.

In addition to ECC Application Profiles linking feature requirements to services, one or more ECC User Accessibility Profiles may be present where the ECC User Accessibility Profile indicates card features not specifically listed in any ECC Application Profile and therefore not essential for interoperable ECC service delivery but which may improve the accessibility to services and/or the usability of the ECC.

An ECC Card Profile may or may not be present but if present offers a convenient way to identify and access other Profiles on the card. It is made up of one or more ECC Application Profiles with their associated electrical interfaces and possibly one or more ECC User Accessibility Profiles. In addition, it may also contain an ECC Durability Profile which contains information relating to the card's durability performance determined according to ISO/IEC 24789 methodology.

An ECC Layout Profile may also be present and indicates the card body features.

Taken together, the use of ECC Profiles will:

— simplify the identification of availability versus requirements of interoperability services;

— cover the whole range of use cases for the ECC;

— provide a sufficient level of flexibility for the card specification;

— enhance the ability of the user to access services according to its personal preferences;

— guarantee the in-field capability and reliability of the card.

The advantages brought about by the specification of these ECC Profiles are clear, however, the specification of profiles is purely optional. In order for a card to comply with the ECC standard the only condition is the implementation of the mandatory requirements of ECC-1 and -2.

Table 1 details in which part of the ECC standard each profile is described: