SLOVENSKI STANDARD
SIST-TS CEN/TS 15480-4:2012

01-maj-2012

Sistemi z identifikacijskimi karticami - Kartica evropskih državljanov - 4. del: Priporočila za izdajanje, delovanje in uporabo kartic evropskih državljanov

Identification card systems - European Citizen Card - Part 4: Recommendations for European Citizen Card issuance, operation and use

Identifikationskartensysteme - Europäische Bürgerkarte - Teil 4: Empfehlungen für Ausgabe, Arbeitsweise und Benutzung der Europäischen Bürgerkarte

Systèmes de cartes d’identification - Carte Européenne du Citoyen - Partie 4: Recommandations pour l’émission, l’exploitation et l’utilisation de la Carte Européenne du Citoyen

Ta slovenski standard je istoveten z: CEN/TS 15480-4:2012

ICS:

35.240.15	Identifikacijske kartice in sorodne naprave	Identification cards and related devices

SIST-TS CEN/TS 15480-4:2012 **en,fr,de**

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN/TS 15480-4

March 2012

ICS 35.240.15

English Version

Identification card systems - European Citizen Card - Part 4: Recommendations for European Citizen Card issuance, operation and use

Systèmes de cartes d'identification - Carte Européenne du Citoyen - Partie 4: Recommandations pour l'émission, l'exploitation et l'utilisation de la Carte Européenne du Citoyen

Identifikationskartensysteme - Europäische Bürgerkarte - Teil 4: Empfehlungen für Ausgabe, Arbeitsweise und Benutzung der Europäischen Bürgerkarte

This Technical Specification (CEN/TS) was approved by CEN on 23 January 2012 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, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: Avenue Marnix 17, B-1000 Brussels

Contents

Foreword

This document (CEN/TS 15480-4:2012) 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.

CEN/TS 15480 "*Identification card systems — European Citizen Card*" consists of the four following parts:

Part 1: Physical, electrical and transport protocol characteristics;

Part 2: Logical data structures and card services;

Part 3: European Citizen Card Interoperability using an application interface;

Part 4: Recommendations for European Citizen Card issuance, operation and use.

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, Turkey and the United Kingdom.

1 Scope

CEN/TS 15480-4 recommends card issuance and operational procedures including citizens' registration.

CEN/TS 15480-4 gives recommendations with regard to the end-user e.g. with respect to privacy and accessibility aspects.

CEN/TS 15480-4 also identifies a set of standard ECC card profiles (e.g. National ID Card, Health Card, Card issued by a Municipality), that can be used as basis for the specification of new ECC projects.

For each profile, this Technical Specification uses a specified template which

— selects a subset of technical requirements from CEN/TS 15480-1, CEN/TS 15480-2:2011 and CEN/TS 15480-3:2010.

— considers the operation of the ECC in its particular environment.

The target audience of CEN/TS 15480-4 is the card issuer.

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 15480-1, *Identification card systems — European Citizen Card — Part 1: Physical, electrical and transport protocol characteristics*

CEN/TS 15480-2:2011, *Identification card systems — European Citizen Card — Part 2: Logical data structures and card services*

CEN/TS 15480-3:2010, *Identification card systems — European Citizen Card — Part 3: European Citizen Card Interoperability using an application interface*

ISO/IEC 12905:2011, *Integrated circuit cards — Enhanced Terminal Accessibility using cardholder preference interface*

3 Abbreviations

For the purposes of this document, the following abbreviations apply.

ARIS	Applicant Registration and Issuance System
ECC	European Citizen Card
EMS	ECC management system
ID card	Identification Card
IVAS	Identity Authentication and Verification System
MRTD	Machine Readable Travelling Document
PKI	Public Key Infrastructure

4 General recommendations on card issuance and operational procedures

4.1 Initial considerations for an ECC project

CEN/TS 15480-4 does not aim at providing an overall solution on how to design and run a complete EMS. It provides some guidance to overcome common challenges that the organisations responsible for the conception and management of the system are likely to face, including the following issues.

- Clear identification of the main purposes of the system and of the nature of the assets to be protected shall lead to the early definition of the security policy to run the system

  The ECC may be issued for different purposes: it can act for example as a national ID card, travelling card, e-government or health insurance card. Following its intended purpose, the EMS main purpose can diverge: to enhance security, to increase efficiency in the provision of services, to reduce identity fraud or to cut expenses by establishing a system of privileges upon card and user's authentication. It is assumed that privacy protection is a common objective. The use cases will define the applications to be selected by the card. In this Technical Specification, use cases translate into ECC profiles (see Annex A), that precisely describe card security mechanisms.

  The practical work of the project can be summarized in the next four points:

  - the analysis of risks based on the ECC use case;
  - the definition of security policies to minimize the impact of those risks;
  - the integration of those security policies within a modular architectural framework;
  - the choice of technologies for implementation of the modules and of the communication interfaces between the system components.

- A secure, trusted and cost-effective scheme should be carefully studied in order to make the appropriate decisions for the inevitable trade-offs in terms of security / cost and security / privacy.

  The ECC provisions have been specified having in mind the system integrator once the system objectives have been set. For instance CEN/TS 15480-3:2010 provides guidance in relation with the key choices relative to the physical and logical distributions of functionalities, the security architecture model and the definition of interfaces for interoperability. The architectures proposed in this Technical Specification, are aimed at avoiding unnecessary system complexity.

- An early decision is the sharing of the security functions between the components of the EMS and the type of e-government services to be provided and their associated risks. Then there are two key issues:

  - to identify the case for strong authentication requiring access to card services;
  - to grant access or not to these services by cardholders external to the domestic system. Then to set the access conditions.

  Cross-Border access represents a case for strong authentication. The scheme can be able to trust a non-domestic e-identity with a similar level of confidence to that of an e-identity issued by the system itself. Transparent access to an e-government server, using the ECC as an authenticator, requires some degree of harmonization between the infrastructures. This Technical Specification encourages deployment of middleware-based access to services according to CEN/TS 15480-3:2010 provisions. This architecture is intended to support the interoperability of electronic identity credentials.

  Clearing and settlement infrastructures for cross-border e-government services are out of the scope of this Technical Specification.

- Trust on e-identity requires confidence on the enrolment and issuance processes through, for instance, the use of the same or similar practices.

  A set of recommendations is provided in 4.4.2 ff. The EMS should be constructed of separate modules. Each module performs its own function. The solution should be device/equipment independent so that personalization equipments from several machinery suppliers may be considered.

  One way to capitalize past investment is by the introduction of a module in the enrolment subsystem able to authenticate and read an electronic document (as an electronic passport) in order to verify the applicant’s identity at the beginning of the enrolment process

  At present, limited harmonization exists at European level and significant differences remain between EU Member States about privacy requirements. ID card issuance and operation is at present under national laws that can differ substantially. Notice as well the lack of legal basis for the cross-border recognition of electronic identities.

  However, EU legislation might be relevant for the ECC which regards the following:

  - data protection during the personal data capture, personalisation, issuance, and operational process, including card renewal. Subclauses 5.1 ff. introduce this issue;

  - the core identification, authentication and digital signature supported by the card that shall comply with European Directive 1999/93/EC [2];

  - the services provided by the card: The ECC is intended to facilitate access to cross-border shared e-Government services as well as to simplify and strengthen the right of free movement and residence of all EU citizens. In that respect, references to the European Directive 2006/123/EC [5] as well as to the European Directive 2004/38/EC [4] are relevant.

  Performing an EMS Private Impact Assessment can help to early identify potentially conflicting procedures. In addition, to make a transparent communication campaign clearly explaining how personal data will be collected and secured with both confidentiality and integrity can help overcome public reluctance and gain social acceptance.

  Privacy concerns for the enrolment and issuance process are described in 5.1 ff. ECC applicants should be provided with full disclosure of the intended use of the ECC credentials and how the related privacy implications are handled.

- Return on Investment is an issue and an early evaluation of cost is needed

  Once the business case is set, cost estimates for public expenditure over a significant period of time (5/10 years, e.g., lifetime of an ECC for ID) is needed. Whilst protection of some assets/fight against fraud/national security may be a business case by itself, the ECC opens the way for collaboration between the private sector and the public administrations. That way costs associated with the deployment and maintenance of the EMS might be shared. That can be achieved by authorizing the use of the card for daily life identification, enable the storage of other e-ID credentials or by using existing communication infrastructures (e.g., authentication infrastructures) for e-government purposes.

  This Technical Specification (Clause 7, Annex A) describes ECC card profiles that cover sound use cases by recommending the use of state-of-the-art technology that will optimize card issuance costs.

- Consider social acceptance since the beginning: ECC management systems shall not discriminate against citizens and specially those with special needs

  It is recommended that the complete set of uses of the personal data stored in the card be disclosed. Public debate on the pro’s and con’s of the proposed schemes and early consideration of expressed public concerns specially for use of new technologies can be useful to gain social acceptance for EMS and cards.

The accessibility to the services using the ECC should be guaranteed in terms of adapted rather than standard use interfaces. The approach of the CEN/TS 15480 series is to store in the card itself those information elements to be retrieved using standard procedures that enable the adaptation of the terminal to the needs defined by the citizens themselves. This Technical Specification defines a specific user accessibility profile according to ISO/IEC 12905:2011 as an application intended to describe the user preferences for the Terminal User Interface.

- Testing is an important aspect to consider when fixing the system architecture

  Past experience with MTRDs proves that sound testing specifications are a pre-condition for ECC interoperability.

- Setting appropriate governance rules is key for EMS security

  The objective of EMS governance is to create a set of end-to-end processes that define roles and responsibilities, and create a practical system for decision-making based on audits and measurements specially on the security performances of the system. In that case, governance may focus on security monitoring and data collection and be a part of a more general security policy program.

  Rules for governance and run of the system should be transparent to gain public confidence.

- Evaluate synergies with other machine readable travelling document projects

  There are direct synergies between the systems deployed for issuance and verification of Machine Readable Travelling Documents (MRTD) and ECCs. For many EU countries, it is expected that the database for the ECC will be linked to the passport database to provide a single logical data source. In addition, the current harmonization process for MRTD specifications, including security and testing requirements, can also impact the ECC. Finally, when the ECC is issued as a travelling document, it should be compatible with ICAO specifications according to EU regulations.

  However, it should be underlined that MRTDs are not issued for access to services. Cross-border secure access to e-government services raises issues specific to the ECC:

  - the support of the electronic signature by the ECC,

  - the access to card services through a standard middleware interface,

  with a triplet of legal, technical and security implications, that have to be considered by ECC government issuers.

Table 1 — Impact considerations

	Legal impact	**Technical impact**	**Security impact**
e-Signature	Non-Repudiation Shift of Liability if Compliance with European Directive	Need for PKI Card compliance with CEN/TS 15480-2:2011	Certification of ECC and e-Sign application against a PP for Secure Signature Creation Device
Access to e-Government Services	Need for Cross-Border recognition of electronic identities	Need for Middleware compliant with CEN/TS 15480-3:2010	Certification of ECC against a PP for Authentication

4.2 ECC Management System and ECC lifecycle description

The ECC issuer should implement a suitable ECC management system (EMS) supporting card lifecycle from blank cards through to delivered cards and including all production errors and sample card issuance. The systems should also handle lost and stolen, damaged and revoked cards.

The ECC lifecycle can be divided into seven stages as described below. Stages 1 to 5 are commonly considered part of the Registration & Issuance Phase. Stage 6 corresponds to the operational life of the card, including some possible maintenance operations. Stage 7 ends the ECC lifecycle.

- Stage 1: Initiation of Card Issuance

  Depending on the ECC scheme, this stage can be started either on a voluntary basis by the citizen or by a mandatory requirement of the administration.

- Stage 2: Citizen Identity Proofing

  The public administration or a third organization under its responsibility (registration authority) identifies the citizen based on the identity-evidence provided

- Stage 3: Identity Credential Issuance

  Based on the authenticated ID attributes of the applicant, the authorized entity issues the e-ID credential, which provides a user identifier to the system. For the ECC the e-ID credential is an electronic certificate and the credentialing authority is a PKI certification authority (CA). The citizen becomes the only legitimate owner of the ID credential during the period of validity of the electronic document.

- Stage 4: ECC Personalization

  The Personalizing Authority stores securely the e-ID credential into the ECC. Along with the identity credential, authenticators needed for the provision of IAS services are also personalized. They can include one or more PIN codes, biometrics and private keys possibly both asymmetric and symmetric.

- Stage 5: ECC Delivery to the Subscriber

  The ECC legitimate user may be subject to a specific authentication procedure by the card issuer before delivery. The ECC standard assumes that not all the card mandatory functionalities may be available at the time of the card delivery, meaning that they may be activated later on, during the operational life stage.

- Stage 6: ECC Operational Life

  The ECC delivery means that the card enters the operational state of its life. The ECC enables the citizen to access the services available. Dependent on the security policy implemented by the ECC issuer authority different card maintenance processes can take place during the operational life of the card. They include

  - activation of card functionalities already present at the time of the ECC delivery,
  - possible renewal of cryptographic information objects, keys and certificates,
  - application downloading after card issuance.

- Stage 7: ECC termination and subsequent renewal

  Scenarios other than the expiration date can lead to termination of the ECC: card stolen or lost, or decision on certification revocation due to possible compromise or misuse. Renewal policies (new issuance of certificates and cards for cardholders) and practices are not covered by this Technical Specification.

  Different EMS subsystems typically interact with the ECC at the different stages of the card operational life. A possible modular implementation of the EMS is presented in 4.3.

4.3 ECC Management System functional organization

The implementation of processes described in 4.2 can be ensured through the deployment of an ECC Management System (EMS) made up of three basic subsystems or primary components which are in turn divided into modules.

The EMS defines rules to combine these modules and securely deliver services. In this subclause, these services are the citizens' registration, including ECC issuance and the citizens' access to on-line services. Furthermore, the technological solutions adopted to implement the modules should ideally be device/equipment independent.

The EMS is made up of three primary subsystems:

1) the ECC card,

2) the Applicant Registration and Issuance System (ARIS) and

3) an Identity Authentication and Verification System (IVAS).

These first-level subsystems are in turn made up of primary functional components.

- The ECC, specified in ECC parts 1 and 2, can be issued selecting one of the application profiles as per Annex A of this document and personalized with data structures enabling access to e-government services using an infrastructure based on ECC part 3.
- The ARIS is made up of four different primary components:
  - enrolment subsystem;
  - card manufacturing and personalization subsystem;
  - PKI subsystem;
  - card issuance subsystem.

- The IVAS, whose core are Authentication Servers and which includes /or is interconnected with a PKI is made up of
  - an IT infrastructure for access to services using the ECC and a standard middleware, proposed in CEN/TS 15480-3:2010,
  - a Web Server infrastructure hosting Applications to grant e-Services accessible through the ECC, the Web Browser and the middleware,
  - a system to detect security/functional incidents and providing with a disaster recovery system.

  The IVAS is briefly introduced in 4.4.3. The architecture of this functional model is based on CEN/TS 15480-3:2010.

Some of these primary components may be shared following the architectural choices.

- PKI Infrastructure may be common to the ARIS and the IVAS.
- A register, database of ECC numbers issued and associated to cardholder personal information (e.g., name), which is fed by the ARIS and is accessed by the IVAS.