PD CEN/TS 15480-5:2013

BSI Standards Publication

Identification card systems — European Citizen Card

Part 5: General Introduction

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

raising standards worldwide™

National foreword

This Published Document is the UK implementation of CEN/TS 15480-5:2013.

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.

© The British Standards Institution 2013

Published by BSI Standards Limited 2013

ISBN 978 0 580 80141 9

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 31 May 2013.

Amendments issued since publication

Amd. No.	Date	Text affected

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

© 2013 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

Ref. No. 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.

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.

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:

Table 1 — Location of ECC Profile Description

Part of the ECC Standard	Durability Profile	Layout Profile	Application Profile	Application Discovery Profile	User Accessibility Profile	Card Profile
ECC-5	Purpose, Definition and Rules for Profile Usage					
ECC-1	X	X				
ECC-2			X			
ECC-3				X		
ECC-4					X	X

6.3.3 Relationship between ECC Profiles

The relationships between ECC Profiles discussed above are illustrated in Figure 1:

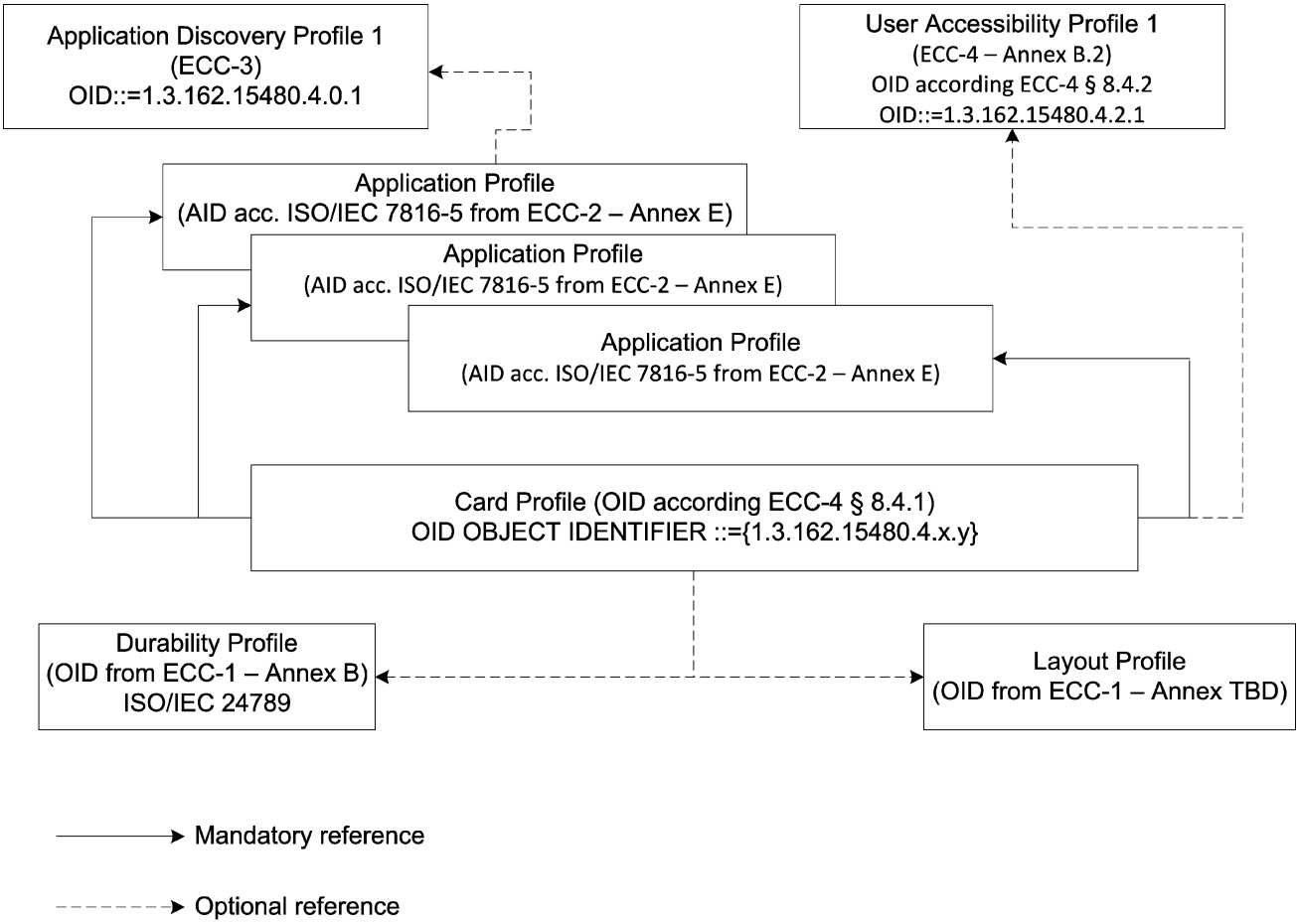

Figure 1 — ECC Profiles relationships

6.3.4 Example of the usage of an ECC Card Profile

The ECC issuer may use the same Card Profile with different card-applications. The Card Profile unique identifier informs the terminal about the type of card platform and so allows the terminal to recognise which Application Profile(s) can be present on such a card and through this matching, the terminal can initialise the appropriate set of functions to handle a transaction with this card.

6.3.5 Example of the usage of an ECC Application Discovery Profile

Specifying a Application Discovery Profile is relevant whenever the issuer wants to have all or part of the card-applications acting in an ISO/IEC 24727-framework as set down in ECC Part 3.

For example, consider the use of a Card Profile which includes two Application Profiles referring respectively to two card-applications. The issuer may select one or both of the two card-applications to run within an ISO/IEC 24727-framework. In addition, the issuer may opt for only part of a selected card-application's features to be exposed to the discovery mechanism. In order to achieve this, the issuer will take the steps as listed below and detailed in part 3 of the ECC standard:

— selection of a method for card discovery;

— implementation of the selected method to publish the registry allowing card discovery;

— since the terminal identifies the ISO/IEC 24727 enabled card application linkages may now be made to that application in one of a variety of methods as described in part 3 of the ECC standard.

Once the measures above are completed, the card can be considered as fitting in with ISO/IEC 24727 middleware.

6.3.6 Example of usage of an ECC User Accessibility Profile

User Accessibility Profiles are needed to determine the set of features and data structures that are to be supported by a card to meet ISO/IEC 12905 [4] requirements for user accessibility. They are assigned OBJECT IDENTIFIERs (OID) for the purpose of their discovery by the terminal as described in ECC Part 4, The terminal may look up the OID values in different ways: either from a normalised information file or from within a dedicated application when present on-card, in both cases, the Profile is said Global to the card. In case the Profile is recoverable from within an application other than the dedicated one, it is said specific to this application.

7 Requirements and options

This standard specifies an ECC that meets the following requirements:

— identification and authentication of the holder by electronic means using reference data stored in the card and also by visual inspection or an appropriate device;

— mutual authentication where required between the card and the terminal communicating with the card;

— secure transmission of data using contact and/or contactless interfaces;

— confidential exchange of data if required;

— electronic signature generation and verification;

— access control mechanisms to stored data;

— the surface of the card shall allow customisation by public administrations to suit their own requirements;

— surface and print security techniques shall be in evidence (or example, holograms and photographs);

— cards shall be resistant to physical attack;

— cards shall provide the capability to support interoperability with other key standards as well as co-exist in environments supporting certain legacy applications;

— cards shall be capable of fitting in with the procedures and policies of the public administrations making use of the ECC;

and optionally:

— multi-application capability;

— post-issuance loading and deleting of applications on the card;

— controlled updating of electronically stored data.

8 Part 1: Physical, electrical and transport protocol characteristics

8.1 General

Part 1 of the ECC standard defines the characteristics of a public service card which may be summarised as follows:

— the ECC is a personalised smart card with an ID-1 format as per ISO/IEC 7810 and a module compliant with the ISO/IEC 7816 parts 1 and 2;

— the card includes:

  i. a contact interface;

  ii. or a contactless interface;

  iii. or a combination of both;

— when the ECC logical data set is compliant with ICAO Doc 9303 specification, then the ECC shall include a contactless interface compliant with ICAO requirements;

— the ECC shall serve to verify the identity of its holder electronically by using identity credentials securely stored in the card memory and possibly using visual features on the card;

— physical characteristics are specified to identify this card as an ECC, provide adequate visual security checking while allowing public administrations to tailor the card visual characteristics to meet their own requirements.

The relevant features described in this part of the ECC standard:

— define low level communication requirements;

— enable its holder to access local and/or remote procedures, transmissions and services made available by the public administration;

— enable visual inspection by suitable technological means;

— are designed for easy evaluation and identification using only the naked eye;

— participate in offering stringent security to match the level of the threat of fraud.

The card should reflect sufficiently the outcome of any national global risk analysis according to national policy incorporating:

— visual identification risks;

— natural or accidental risks;

— fraud or counterfeiting risks and risks linked to the voluntary degradation of the protective covering and integrated circuit chip module.

8.2 Compliance with public administration requirements and citizen expectations

The ECC shall comply with the respective public administration requirements and in so doing shall:

— simplify the administrative handling of official document requests and provides the means to ensure the full integrity of processed and transmitted information;

— provide standard and reliable means of visual identification where systematic access to specific readers proves difficult;

— support the specific visual requirements of the public administration;

— provide adequate citizen privacy protection.

8.3 Identifying an ECC holder

A link between the ECC and its holder is essential to avoid the ECC being used by a third party and to prevent this third party illegally using a found or stolen ECC as well as to avoid any text or graphics from being modified for fraudulent or improper use. In general both electronic and physical means will be used depending upon the usage environment and circumstances:

— physical identification will include a photograph and signature of the holder on the card may be mandatory together with an identification number and civil status data depending upon the requirements of the public administration;

— electronic identification is implemented through the mechanisms specified in ECC-2.

9 Part 2: Logical data structures and card services

This part of the ECC standard specifies the logical characteristics and security features at the card/system interface for the European Citizen Card which, since it is a smart card with Identification, Authentication and electronic Signature (IAS) services requires that:

— the supported services are specified;

— the supported data structures as well as the access to these structures are specified;

— the command set is defined.

This part of the ECC standard has the objective of ensuring the interoperability at card/system interface in the usage phase. In order to reach the interoperability objective, IAS services are compliant to EN 14890-1 and EN 14890-2. Since the EN documents offer options, this part of the ECC standard includes a specification of the options to be used in order to define a complete profile.

Part 2 also provides other features not defined in the EN documents (for example, on-card biometric comparison, and command chaining and role authentication). It will also allow an ICAO specification to be loaded since it supports the necessary requirements such as authentication methods and basic access control.

The use of a particular platform is not mandated, which allows both native and Java card technologies to be used.

This specification encompasses mandatory and optional features.

— Mandatory features must be implemented on a smart card to be compliant to this standard.

— Optional features make up a toolbox of modular options from which issuers can pick up the necessary protocols to fulfil the requirements of their use cases including an optional set of ECC Application Profiles from which they can refer to the most appropriate.

The standard provides that two ECC compliant IAS-enabled smart cards issued by two different issuers and implementing different specified modular options, can interoperate with a terminal provided that the terminal supports both options, including the command sets used. Therefore, interoperability requires a specific agreement between issuers/governments in order to determine which cross-border services are to be shared, and consequently which protocols are to be supported by the terminals in each country.

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

10.1 General

Different Member State's public administrations may or may not offer e-services in an ISO/IEC 24727 environment. ISO/IEC 24727 is a standard offering a unified approach to e-service provision involving the use of smart cards as access tokens and/or application dependent tokens. Older legacy systems will not conform to ISO/IEC 24727 while newer ones may do so. Part 3 of the European Citizen Card standard is intended to provide middleware solutions to allow interoperability with both environments.

While it would be possible to use ISO/IEC 24727 directly without employing the ECC standard, the card level interoperability offered by the ECC would not be achievable. In addition, the ECC standard parts 1 and 2, on their own, are not sufficient to interface properly with ISO/IEC 24727. Part 3 of the ECC standard fills this gap. It also provides:

— improvements to e-Service implementation by sparing to the Client-Application the need to handle intricate encoded data;

— optimisation and completion of the interface controlling the readers;

— updating and maintenance of the containers involved in the discovery mechanism;

— management of Post-issuance personalisation calls with an additional specification fixing all the details and clearing pending ambiguities;

— integration into federated ID systems (such as Liberty Alliance, TLS-Federation, WS-*, etc).

And other detail level benefits.

ECC-3 is intended for both:

— smart card Issuers who want to offer to their end-users secure access to shared e-Services;

— middleware suppliers who want to interconnect ECCs with shared e-Services through an innovative middleware technology enabled via a discovery mechanism to avoid the common restriction of a one-to-one e-Service and card relationship.

10.2 Tools for smartcard suppliers

For ECC-compliant cards to access shareable e-Services (such as web services) in a secure manner:

— during the migration path from the various existing e-Administration, e-Id or e-Government specifications to the ECC, technical arrangements are necessary to facilitate support for legacy cards so that holders of such cards can access the same e-Services as holders of ECC cards;

— when present, they have to fit into a framework designed upon ISO/IEC 24727 and allow for recognition of cards from different vendors.

This part of the ECC standard provides the means for legacy card support and will allow one Member State's ECC card to interoperate with another European ECC subject to agreement between the Member States and provided that all the cards' low level features correspond to relevant ISO standards.

Part 3 of the ECC standard provides card issuers with recommendations and implementation guidelines to personalise newly released cards or to adapt existing cards so that they can offer access to a shared e-Service. For example, they can find:

— how to prepare meta-language descriptors for the support of their legacy cards;

— how to encode their ISO/IEC 24727 card containers to render their cards discoverable by the ECC service layer;

— how to indicate an ECC User Accessibility Profile on their cards;

— how to encode the authentication protocols protecting their card services and assets to ensure its interpretation by ECC part 3 middleware;

— how to store discovery data structures on their cards so that existing personalisation items may be reused;

— how to create a new service on existing cards by exposing all or part of their card features (functions and data) to the ECC part 3 service layer.

10.3 Tools for integrators

Middleware suppliers can find recommendations and implementation guidelines to claim ISO/IEC compatibility with enhancements for ECC cards. For example, they can find:

— how to implement an optimised service layer decision tree;

— how to interpret the discovery data denoting the authentication protocol, if any, supported by their cards operating within an ISO/IEC 24727 framework;

— how to process post-issuance personalisation requests on cards;

— how to support legacy cards, how to recognise an ECC part 4 compliant Profile whenever such profile is implemented by an embedded card-application;

— how to access enhanced readers by implementing a generic interface device API;

— how to ensure accordingly an interoperable implementation of this API;

— how to allow transaction between a Web Service and a remote reader;

i. how to improve the e-Service implementation by avoiding the requirement for the Client-Application executing this e-Service to handle intricate encoded data; how to exploit a meta-language-based script to replace the byte-code recommended by ISO/IEC 24727 for the translation of generic card commands into card-specific commands;

ii. how to build an architecture with a distributed middleware for an optimised deployment based on ISO/IEC 24727 recommendations.

10.4 Compatibility with other standards

The scope covered by ECC-3 overlaps a part of ISO/IEC 24727 as described in Figure 2. A shortlist of features from ISO/IEC 24727 were adopted by ECC-3 that ensure compatibility with the ISO standard, whereas other features are rather ECC-3 specific. A harmonisation effort was conducted by an ECC-3 ad hoc group before the ISO/SC17/WG4 committee in order to have those ECC-3 extra features endorsed by ISO/IEC 24727.

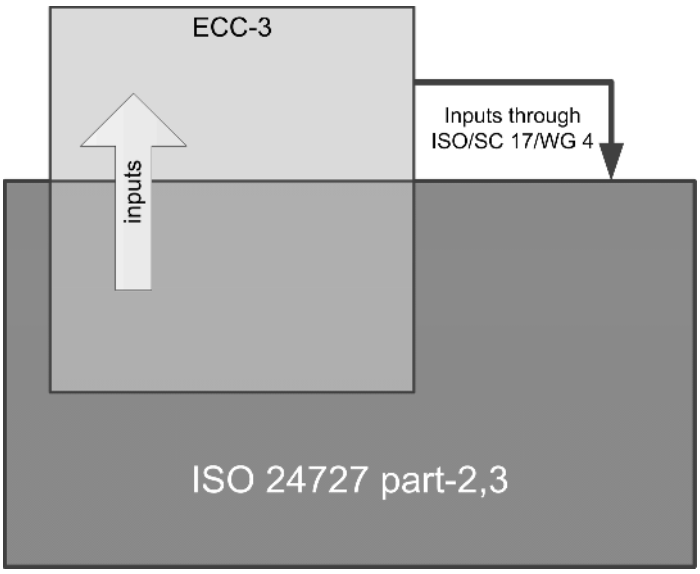

Figure 2 — intersection between ECC-3 coverage and ISO/IEC 24727

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

Part 4 recommends card issuance and operational procedures including citizen registration.

Part 4 gives recommendations with regard to the end-user e.g. with respect to privacy and accessibility aspects.

Part 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 the standard uses a specified template which

— selects a subset of technical requirements from CEN/TS 15480-1, CEN/TS 15480-2 and CEN/TS 15480-3;

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

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

Part 4 of the ECC standard recommends a variety of approaches to best support the cardholder because experience shows that the success of applications whose use is voluntary by the citizen depends very much on the acceptance of the citizen including transparency of the processes involved, the ease of issuance, the method of card use and the surrounding operational procedures. Acceptance by the citizen is influenced by the adherence to accessibility, usability, privacy and health and safety principles. Nevertheless an added value for the use of a technology needs to be evident and clear to the citizen. A citizen not accepting the technology will decide not to use it. In addition, for applications whose use is mandatory by the citizen, acceptance is an important factor, as the performance of an application depends on the citizen being cooperative.

Nevertheless, recommendations on card issuance and operational procedures are given at a general level as the ECC can mean many different things and be used in many different environments, so there cannot be a single mechanism specified for setting up card issuance, application definition and operational procedures. The power of the ECC is that a single standard can cover many environments and application usage scenarios. Therefore the recommendations are set down at a general level to allow the implementer to select the most appropriate for them and in the knowledge of local national legislation which may affect or mandate different options.

Annex A
(informative)

Relationship between ECC standard parts and ISO standards

A.1 Mapping of ECC to ISO standards

Figure A.1 provides a functional layout description to mapping the ECC series of parts of its standard with some outstanding card platform ISO/IEC Standards.

The particular ubiquitous role of ISO/IEC 7816-15 is such as several other standards are built on it. For example, in the case of the ECC, ECC Part 2 shall resort to ISO 7816-15 to ensure interoperability between different ECC implementations through cryptographic objects' attributes description; whilst ECC Part 4 may resort to ISO/IEC 7816-15 for data object description and cross-referencing between Application Profiles and Card Profiles; and ECC part 3 may rely on ISO 7816-15 for Target (acc. ISO/IEC 24727 definition for *Target*) mapping onto ISO/IEC 7816-15 attributes as a provision for the discovery mechanism.

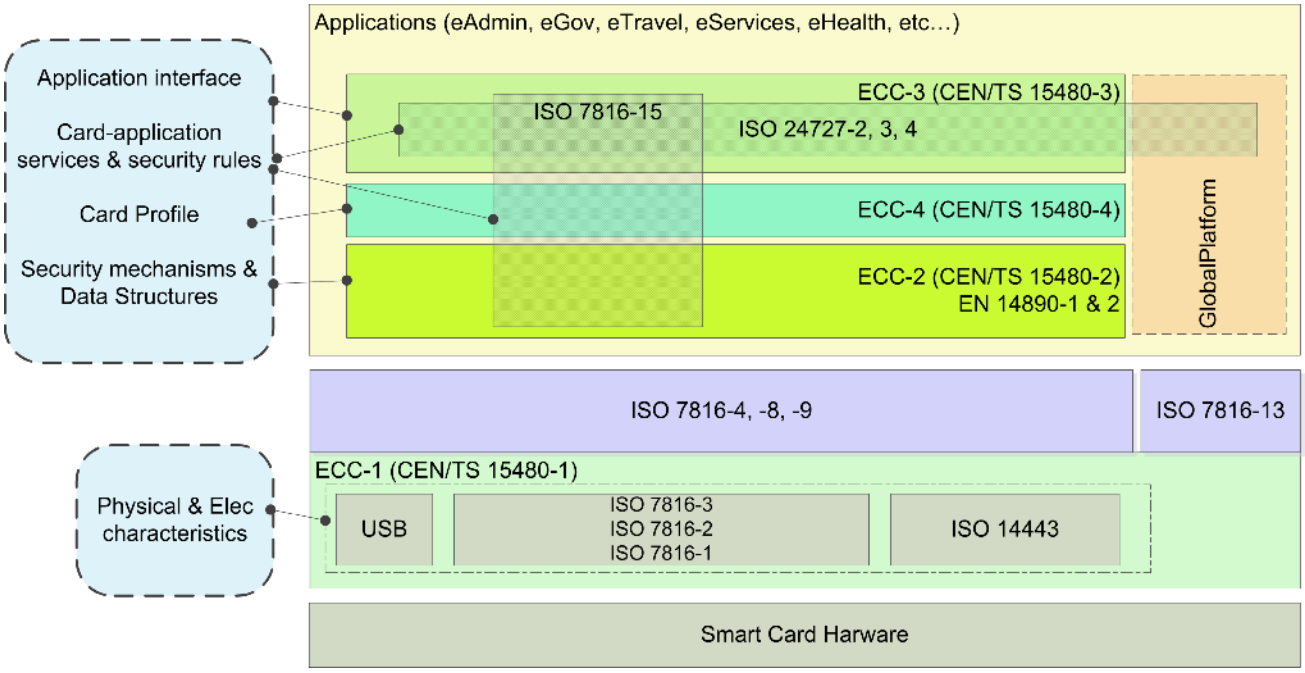

Figure A.1 — Card platform standards bricks

Bibliography

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

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

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

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

[5] EN 14890-1, *Application Interface for smart cards used as Secure Signature Creation Devices — Part 1: Basic services*

[6] EN 14890-2, *Application Interface for smart cards used as Secure Signature Creation Devices — Part 2: Additional Services*

[7] ISO/IEC 12905, *Integrated circuit cards — Enhanced Terminal Accessibility using cardholder preference interface*

[8] ISO/IEC 24727 (all parts), *Identification cards — Integrated circuit card programming interfaces*

[9] ISO/IEC 7816 (all parts), *Identification cards — Integrated circuit(s) cards with contacts*

[10] ISO/IEC 14443 (all parts), *Identification cards — Contactless integrated circuit cards — Proximity cards*

[11] ISO/IEC 24789 (all parts), *Identification cards — Card service life*

[12] ISO/IEC 7810, *Identification cards — Physical characteristics*

[13] ISO/IEC 7816 (all parts), *Identification cards — Integrated circuit(s) cards with contacts*

This page deliberately left blank

British Standards Institution (BSI)

BSI is the independent national body responsible for preparing British Standards and other standards-related publications, information and services. It presents the UK view on standards in Europe and at the international level.

BSI is incorporated by Royal Charter. British Standards and other standardisation products are published by BSI Standards Limited.

Revisions

British Standards and PASs are periodically updated by amendment or revision. Users of British Standards and PASs should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using British Standards would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover. Similary for PASs, please notify BSI Customer Services.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001

BSI offers BSI Subscribing Members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of British Standards and PASs.

Tel: +44 (0)20 8996 7669 Fax: +44 (0)20 8996 7001
Email: plus@bsigroup.com

Buying standards

You may buy PDF and hard copy versions of standards directly using a credit card from the BSI Shop on the website **www.bsigroup.com/shop.** In addition all orders for BSI, international and foreign standards publications can be addressed to BSI Customer Services.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001
Email: orders@bsigroup.com

In response to orders for international standards, BSI will supply the British Standard implementation of the relevant international standard, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Knowledge Centre.

Tel: +44 (0)20 8996 7004 Fax: +44 (0)20 8996 7005
Email: knowledgecentre@bsigroup.com

BSI Subscribing Members are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration.

Tel: +44 (0)20 8996 7002 Fax: +44 (0)20 8996 7001
Email: membership@bsigroup.com

Information regarding online access to British Standards and PASs via British Standards Online can be found at **www.bsigroup.com/BSOL**

Further information about British Standards is available on the BSI website at **www.bsi-group.com/standards**

Copyright

All the data, software and documentation set out in all British Standards and other BSI publications are the property of and copyrighted by BSI, or some person or entity that own copyright in the information used (such as the international standardisation bodies) has formally licensed such information to BSI for commerical publication and use. Except as permitted under the Copyright, Designs and Patents Act 1988 no extract may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior written permission from BSI. This does not preclude the free use, in the course of implementing the standard, of necessary details such as symbols, and size, type or grade designations. If these details are to be used for any other purpose than implementation then the prior written permission of BSI must be obtained. Details and advice can be obtained from the Copyright & Licensing Department.

Tel: +44 (0)20 8996 7070
Email: copyright@bsigroup.com

BSI

389 Chiswick High Road London W4 4AL UK

Tel +44 (0)20 8996 9001
Fax +44 (0)20 8996 7001
www.bsigroup.com/standards

raising standards worldwide™