



SLOVENSKI STANDARD
SIST-TS CEN/TS 15480-1:2009
01-februar-2009

GjghYa]n]XYbhZ_UW'g_]a]_Ufh]WLa]!'?Ufh]WUj] fcdg_]\`XfyUj`^Ubcj`!'%'XY.
:]n] bYžYY_f] bY]b`fUbgdcf]bY'nbU]bcgh]dfc]c_c`U

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

Identifikationskartensysteme - Europäische Bürgerkarte - Teil 1: Physikalische, elektrische und transportprotokollbezogene Merkmale

Systèmes des cartes d'identification - Carte Européenne du Citoyen - Partie 1: Caractéristiques physiques, électriques et protocoles de transmission

<https://standards.iteh.ai/catalog/standards/sist/29f8e28b-a7fd-43ba-ba0c-b2a8b4236d8f/sist-ts-cen-ts-15480-1-2009>

Ta slovenski standard je istoveten z: CEN/TS 15480-1:2007

ICS:

| | | |
|-----------|---|--|
| 35.240.15 | Identifikacijske kartice in sorodne naprave | Identification cards and related devices |
|-----------|---|--|

SIST-TS CEN/TS 15480-1:2009 **en**

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SIST-TS CEN/TS 15480-1:2009](https://standards.iteh.ai/catalog/standards/sist/29f8e28b-a7fd-43ba-ba0c-b2a8b4236d8f/sist-ts-cen-ts-15480-1-2009)

<https://standards.iteh.ai/catalog/standards/sist/29f8e28b-a7fd-43ba-ba0c-b2a8b4236d8f/sist-ts-cen-ts-15480-1-2009>

TECHNICAL SPECIFICATION
SPÉCIFICATION TECHNIQUE
TECHNISCHE SPEZIFIKATION

CEN/TS 15480-1

April 2007

ICS 35.240.15

English Version

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

Systèmes des cartes d'identification - Carte Européenne du
Citoyen - Partie 1: Caractéristiques physiques, électriques
et protocoles de transmission

Identifikationskartensysteme - Europäische Bürgerkarte -
Teil 1: Physikalische, elektrische und
transportprotokollbezogene Merkmale

This Technical Specification (CEN/TS) was approved by CEN on 17 July 2006 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, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

[SIST-TS CEN/TS 15480-1:2009](https://standards.iteh.ai/catalog/standards/sist/29f8e28b-a7fd-43ba-ba0c-b2a8b4236d8f/sist-ts-cen-ts-15480-1-2009)

<https://standards.iteh.ai/catalog/standards/sist/29f8e28b-a7fd-43ba-ba0c-b2a8b4236d8f/sist-ts-cen-ts-15480-1-2009>



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

Management Centre: rue de Stassart, 36 B-1050 Brussels

CEN/TS 15480-1:2007 (E)

| Contents | Page |
|--|-------------|
| Foreword..... | 3 |
| Introduction | 4 |
| 1 Scope | 5 |
| 2 Normative references | 5 |
| 3 Terms and definitions | 6 |
| 4 Symbols and abbreviations | 12 |
| 5 Definition, use and functions of the European Citizen Card (ECC) | 13 |
| 5.1 General | 13 |
| 5.2 Compliance with public administration requirements and citizen expectations | 14 |
| 5.3 Citizen privacy protection | 14 |
| 5.4 Identifying a ECC holder | 14 |
| 5.5 European Citizen Cards functions | 15 |
| 6 ECC physical characteristics | 15 |
| 6.1 General | 15 |
| 6.2 Materials | 16 |
| 6.3 ECC physical security elements | 16 |
| 6.4 ECC security evaluation | 18 |
| 7 Electrical characteristics | 18 |
| 7.1 Dimensions and location of the contacts or coupling area | 18 |
| 7.2 The contact interface | 18 |
| 7.3 Contactless interface | 18 |
| 8 Transport protocols | 18 |
| 9 Terminal characteristics | 19 |
| Annex A (informative) General card design (with reference to Directive 96/47/EC relating to European driving licences) | 20 |
| Annex B (informative) Methodology for the design of ECC durability testing | 23 |
| B.1 General | 23 |
| B.2 Introduction | 23 |
| B.3 Vocabulary | 24 |
| B.4 Methodology for ECC durability | 24 |
| B.5 Core test sequence requirements | 29 |
| B.6 Individual tests relevant for the ECC | 30 |
| B.7 Examples of mission profile calculations for the ECC | 35 |
| Annex C (informative) Security requirements for the ECC as a travel document (Council Regulation on e-passports and travel documents) | 39 |
| C.1 Material | 39 |
| C.2 Biographical data page | 39 |
| C.3 Printing techniques | 40 |
| C.4 Protection against copying | 40 |
| C.5 Issuing technique | 41 |
| Bibliography | 42 |

Foreword

This document (CEN/TS 15480-1:2007) 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.

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

Part 1: *Physical, electrical and transport protocol characteristics*

Part 2: *Logical data structures and card services*

Part 3: *ECC interoperability using an application interface*

Part 4: *Recommendations for ECC issuance, operation and use*

According to the CEN/CENELEC Internal Regulations, the national standards organizations of the following countries are bound to announce this CEN Technical Specification: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

[SIST-TS CEN/TS 15480-1:2009](https://standards.iteh.ai/catalog/standards/sist/29f8e28b-a7fd-43ba-ba0c-b2a8b4236d8f/sist-ts-cen-ts-15480-1-2009)

<https://standards.iteh.ai/catalog/standards/sist/29f8e28b-a7fd-43ba-ba0c-b2a8b4236d8f/sist-ts-cen-ts-15480-1-2009>

CEN/TS 15480-1:2007 (E)

Introduction

This Technical Specification describes the specifications for the European Citizen Card (ECC) including electronic identity cards, with smart card format, defining identity justification with emphasis on remote civil service procedures.

This proposal is intended to comply with the scope of the NWI ECC as defined by the terms of reference document approved by the CEN/TC 224 Resolution 667/2004.

This Technical Specification is one of a set of documents describing card specifications. It defines identity justification functions, with emphasis on remote public service procedures requiring the generation and/or verification by the ECC card of electronic signatures and electronic certificates.

iTeh STANDARD PREVIEW (standards.iteh.ai)

[SIST-TS CEN/TS 15480-1:2009](https://standards.iteh.ai/catalog/standards/sist/29f8e28b-a7fd-43ba-ba0c-b2a8b4236d8f/sist-ts-cen-ts-15480-1-2009)

<https://standards.iteh.ai/catalog/standards/sist/29f8e28b-a7fd-43ba-ba0c-b2a8b4236d8f/sist-ts-cen-ts-15480-1-2009>

1 Scope

This Technical Specification specifies Electronic Citizen Card (ECC) requirements. The ECC, is a smart card issued under the authority of a government institution, either national or local and carries credentials in order to provide all or part of the following services:

- 1) verify the identity;
- 2) act as an Inter-European Union travel document;
- 3) facilitate logical access to e-government or local administration services.

A public administration authority may entitle a private organisation to provide all or part of the ECC services.

This Technical Specification is intended to offer the card issuer with a great deal of flexibility for the ECC specification, in connection with the services that the ECC provides, the authentication mechanisms supported and the national specific public policy with an special concern to protect the citizen privacy according to the applicable European legislation.

The requirements described in this Technical Specification are used to:

- a) define a plastic body card with associated physical and logical securities;
- b) specify the electrical interface and data transport protocols for the ECC;
- c) support the basic set of Identification and, authentication elements visible at the card surface.

This Technical Specification also contains a possible methodology for ECC durability testing in informative Annex B.

This Technical Specification refers to the European legislation and regulations in effect.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 7810, *Identification cards — Physical characteristics*

ISO/IEC 7816-1, *Identification cards — Integrated circuit(s) card(s) with contacts — Part 1: Physical characteristics*

ISO/IEC 7816-2, *Identification cards — Integrated circuit cards — Part 2: Cards with contacts — Dimensions and location of the contacts*

ISO/IEC 7816-3, *Identification cards -- Integrated circuit cards -- Part 3: Cards with contacts -- Electrical interface and transmission protocols*

ISO/IEC 7816-4, *Identification cards — Integrated circuit(s) cards — Part 4: Organization, security and commands for interchange*

CEN/TS 15480-1:2007 (E)

ISO/IEC 7816-5, *Identification cards — Integrated circuit cards — Part 5: Registration of application identifiers*

ISO/IEC 7816-6, *Identification cards — Integrated circuit cards — Part 6: Interindustry data elements for interchange*

ISO/IEC 7816-7, *Identification cards — Integrated circuit(s) cards with contacts — Part 7: Interindustry commands for Structured Card Query Language (SCQL)*

ISO/IEC 7816-8, *Identification cards — Integrated circuit cards — Part 8: Commands for security operations*

ISO/IEC 7816-9, *Identification cards — Integrated circuit cards — Part 9: Commands for card management*

ISO/IEC 7816-10, *Identification cards — Integrated circuit(s) cards with contacts — Part 10: Electronic signals and answer to reset for synchronous cards*

ISO/IEC 7816-11, *Identification cards — Integrated circuit cards — Part 11: Personal verification through biometric methods*

ISO/IEC 7816-12, *Identification cards — Integrated circuit cards — Part 12: Cards with contact — USB electrical interface and operating procedures*

ISO/IEC 7816-15, *Identification cards — Integrated circuit cards — Part 15: Cryptographic information application*

ISO/IEC 10373-3, *Identification cards — Test methods — Part 3: Integrated circuit(s) cards with contacts and related interface devices*

ISO/IEC 10373-6, *Identification cards — Test methods — Part 6: Proximity cards*

ISO/IEC 14443-1, *Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 1: Physical characteristics*

ISO/IEC 14443-2, *Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 2: Radio frequency power and signal interface*

ISO/IEC 14443-3, *Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 3: Initialization and anticollision*

ISO/IEC 14443-4, *Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 4: Transmission protocol*

ICAO 9303, Part 1, *Machine Readable Passports*

ICAO 9303, Part 2, *Machine Readable Visas*

ICAO 9303, Part 3, *Machine Readable Official Documents of Identity*

3 Terms and definitions

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

3.1**access control**

mechanism for limiting the use of some ECC resources to authorized users, based on the privilege attributes of the requester and control attributes of the requested resource. Access control mechanisms may be used to protect disclosure of private sensitive data stored in the ECC

3.2**alteration**

fraudulent action of changing a part of an original document, e.g. by changing the biographical data of the document holder

3.3**application**

data structure, data elements and program modules needed for a specific functionality to be satisfied

3.4**authentication**

provision of assurance of the claimed identity of an entity

[ISO/IEC 10181-2:1996]

3.5**authorization**

right or permission that is granted to the ECC holder after its successful authentication

3.6**card holder**

legal holder of the ECC

3.7**card issuing authority**

entity that issues the ECC

3.8**Certification Authority (CA)**

means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures

[Directive 1999/93/EC]

3.9**checking the authenticity of the issuing authority**

- verifying the authenticity of the card,
- verifying that the card is compliant with Civil Service specifications;
- verifying the issuing authority;
- identifying the ECC by its intrinsic properties.

The authenticity inspection may be conducted using resources such as a magnifying glass, UV lamp, digital fingerprint sensor, micromodule reader etc.

iTech STANDARD PREVIEW
(standards.iteh.ai)

[SIST-TS CEN/TS 15480-1:2009](https://standards.iteh.ai/catalog/standards/sist/29f8e28b-a7fd-43ba-ba0c-b2a8b4236d8f/sist-ts-cen-ts-15480-1-2009)

<https://standards.iteh.ai/catalog/standards/sist/29f8e28b-a7fd-43ba-ba0c-b2a8b4236d8f/sist-ts-cen-ts-15480-1-2009>

CEN/TS 15480-1:2007 (E)**3.10****counterfeiting**

unauthorized document that has the same security characteristics as the original document ones and that cannot be distinguished from a legitimate one. For instance a card made from a blank stolen document

3.11**credentials**

known data attesting to the truth of certain citizen identity attributes and stored in the ECC

3.12**electronic certificate**

means an electronic attestation which links signature-verification data to a person and confirms the identity of that person

[Directive 1999/93/EC]

3.13**electronic signature**

means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication

[Directive 1999/93/EC]

3.14**evaluation**

assessment of a PP, an ST or a TOE, against defined criteria

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.15**Evaluation Assurance Level (EAL)**

package consisting of assurance components from ISO/IEC 15408-3 that represents a point on the CC predefined assurance scale

SIST-TS CEN/TS 15480-1:2009

<https://standards.iteh.ai/catalog/standards/sist/298e28b-a7fd-43ba-ba0c-b2a8b4236d81/sist-ts-cen-ts-15480-1-2009>

3.16**fingerprint minutia(e)**

minutiae are characteristics of digital fingerprint ridges (start, end, ridge bifurcation). Each minutia is represented by a mathematical point and an angle defining a position and a direction. Minutiae are represented by a dot map used to single out digital fingerprints and people

3.17**falsification**

refer to alteration and simulation

3.18**fixed administrative information**

general information on an identity document in a predefined, precise order, pre-printed or otherwise, constituting the structure for all personal information contained in the said document

3.19**guilloche**

motifs formed using continuous thin lines, usually created by a computer, together forming a unique image that may only be perfectly reproduced with the same equipment (software, parameters, hardware and materials) used to produce the original motif

3.20**identification**

process necessary to recognise the identity of the cardholder

3.21**identified transaction**

is one in which the data can be readily related to a particular individual, because the transaction carries a credential of the person concerned or because the transaction contains data which, in combination with other available data, links the transaction to a particular person

3.22**initial and secondary ECC examinations**

initial examination is an analysis of the ECC security components either visually and/or using light, transportable resources. A secondary examination is an analysis of ECC security components using laboratory technology resources

3.23**interoperability**

property enabling heterogeneous equipment concerned by electronic exchanges, to inter-communicate in compliance with standards.

These standards specify the following common characteristics:

— electrical and mechanical interfaces;

— structure and coding of exchanged messages;

— data identifiers;

— commands structure and coding for data processing

3.24**machine readable zone**

three lines of OCR-B characters on the back of a ID1 card that may be read by a machine

(see ICAO 9303)

3.25**microcontroller**

electronic component integrating the different physical elements of a card (CPU, ROM, RAM, EEPROM and possibly a cryptoprocessor etc.)

3.26**micromodule**

electronic part of the ECC and includes the integrated circuit and components required to connect to the outside world. There are several micromodule types. The main types are:

— contact micromodule:

this type of micromodule is designed to communicate using embedded mechanical characteristics in compliance with the rules of ISO/IEC 7816;

— contactless micromodule:

ITeH STANDARD PREVIEW
(standards.iteh.ai)

SIST-TS CEN/TS 15480-1:2009

[https://standards.iteh.ai/catalog/standards/sist/29f8e28b-a7fd-43ba-ba0c-](https://standards.iteh.ai/catalog/standards/sist/29f8e28b-a7fd-43ba-ba0c-02a6b4250c6f/sist-ts-cen-ts-15480-1-2009)

[02a6b4250c6f/sist-ts-cen-ts-15480-1-2009](https://standards.iteh.ai/catalog/standards/sist/29f8e28b-a7fd-43ba-ba0c-02a6b4250c6f/sist-ts-cen-ts-15480-1-2009)

CEN/TS 15480-1:2007 (E)

this type of micromodule is designed to allow the card to only communicate using radio frequencies whose characteristics are defined in ISO/IEC 14443;

— mixed micromodule:

this type of micromodule is designed to allow the card to communicate in both contact and contact-less modes via a radio frequency link, whose characteristics are defined in ISO/IEC 14443, with the reader. Cards with this type of micromodule are called “combination cards” or “dual interface cards”

3.27**microlettering**

text with very small font size, printed in positive or in negative and that may be read using a magnifying device

3.28**mission profile**

durability of a card in the field is defined with respect to the “usage” conditions and the “age” criteria. Both are dependant on the environment, storage by the user and the reader profile. Respectively all these parameters are influenced by the frequency of use and the card operational life

3.29**optical variable feature**

image or device whose colour and/or design changes depending on the angle of vision or the amount of light used

3.30**private key**

key of an entity's asymmetric key pair which should only be used by that entity

[ISO/IEC 11770-1:1996]

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SIST-TS CEN/TS 15480-1:2009](https://standards.iteh.ai/catalog/standards/sist/29f8e28b-a7fd-43ba-ba0c-b2a8b4236d8f/sist-ts-cen-ts-15480-1-2009)

<https://standards.iteh.ai/catalog/standards/sist/29f8e28b-a7fd-43ba-ba0c-b2a8b4236d8f/sist-ts-cen-ts-15480-1-2009>

3.31**protection profile**

implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs

3.32**public key**

key of an entity's asymmetric key pair which can be made public

[ISO/IEC 11770-1:1996]

3.33**public key infrastructure (PKI)**

system that uses asymmetric encryption to provide proof of identity, data privacy, non-repudiation and data integrity

3.34**rainbow printing**

technique used to print two or more colours simultaneously to create controlled mixes of colours that vary consistently and gradually between two different zones

— electronic reading/writing zone with contact:

this is determined by the location of the micromodule metallic contacts. The location of this zone is defined by ISO/IEC 7816-2;

- electronic reading/writing zone without contact:

this is determined by the volume associated with the information exchange device in which a card may be read or written by the reader as per ISO/IEC 14443;

- electronic reading/writing zone for a mixed card:

this zone provides the same function as both the contact and contactless electronic communication zones

3.35

physical protection

additional layer applied during the personalization process that protects the variable data of the ECC (e.g. photo) and the ECC card body. They include laminate, overlay, varnish, patches, holograms or any combination of them

3.36

pseudonym

identifier for a party to a transaction, which is not, in the normal course of events, sufficient to associate the transaction with a particular citizen

3.37

pseudonymous transaction

one in which the transaction data contains no direct citizen identifier. The data may however be indirectly associated with the citizen if particular procedures are followed

3.38

remote procedure

paperless exchange of administrative processes between public authorities (ministers, public bodies etc.) and their partners and citizens.

The main stages are:

- request for access to an on-line procedure;
- loading of an on-line procedure;
- loading of procedure-related data;
- filling up of document on screen;
- signature and transfer of procedure-related data

3.39

remote transmission

transmission via a paperless data network of non-secure and secure data (encoding and/or electronic signature)

3.40

ROM

non-volatile, non-rewritable memory technology applicable to operating systems and allowing the storage of all or some software components. Other non-volatile memory technologies can also be used, such as Flash-EEPROM memories

ITeH STANDARD PREVIEW
(standards.iteh.ai)

SIST-TS CEN/TS 15480-1:2009

<https://standards.iteh.ai/catalog/standards/sist/29f8e28b-a7fd-43ba-ba0c-b2a8b4236d8f/sist-ts-cen-ts-15480-1-2009>