



NSAI
Standards

Standard Recommendation
S.R. CEN/TS 15480-2:2012

Identification card systems - European Citizen Card - Part 2: Logical data structures and security services

S.R. CEN/TS 15480-2:2012

Incorporating amendments/corrigenda/National Annexes issued since publication:

The National Standards Authority of Ireland (NSAI) produces the following categories of formal documents:

I.S. xxx: Irish Standard – national specification based on the consensus of an expert panel and subject to public consultation.

S.R. xxx: Standard Recommendation - recommendation based on the consensus of an expert panel and subject to public consultation.

SWIFT xxx: A rapidly developed recommendatory document based on the consensus of the participants of an NSAI workshop.

This document replaces:

This document is based on:
CEN/TS 15480-2:2012
EN 61228:1994

Published:
2 July, 2012
29 September, 1994

This document was published under the authority of the NSAI and comes into effect on:
2 July, 2012

ICS number:

35.240.15

NSAI
1 Swift Square,
Northwood, Santry
Dublin 9

T +353 1 807 3800
F +353 1 807 3838
E standards@nsai.ie
W NSAI.ie

Sales:
T +353 1 857 6730
F +353 1 857 6729
W standards.ie

Údarás um Chaighdeáin Náisiúnta na hÉireann

ICS 35.240.15

English Version

Identification card systems - European Citizen Card - Part 2: Logical data structures and security services

Systèmes de cartes d'identification - Carte Européenne du
Citoyen - Partie 2: structures de données logiques et
services de sécurité

Identifikationskartensysteme - Europäische Bürgerkarte -
Teil 2: Logische Datenstrukturen und Sicherheitsfunktionen

This Technical Specification (CEN/TS) was approved by CEN on 9 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

Page

Foreword.....	4
1 Scope	5
2 Normative references	5
3 Terms and definitions	6
4 Abbreviations	7
4.1 Abbreviations	7
4.2 Coding conventions and notation.....	9
5 Data elements and data structures	10
5.1 Supported data Structures	10
5.2 Access to data structures	10
5.3 Answer to reset (ATR) / answer to select (ATS)	11
5.4 General architecture and file supported	15
5.5 Selection of data structures	16
5.6 Access to files.....	17
6 Basic card services	18
6.1 General.....	18
6.2 Identification.....	18
6.3 User verification.....	20
6.4 Device authentication.....	20
6.5 Digital signature.....	23
6.6 Client/Server Authentication	24
6.7 Encryption key decipherment	24
7 Extended card services.....	25
7.1 General.....	25
7.2 Biometrics – on card matching	25
7.3 Passive Authentication	25
7.4 Basic Access Control.....	25
7.5 Active Authentication.....	25
7.6 Extended Access Control	26
7.7 Role authentication.....	26
7.8 Restricted Identification (RI).....	27
7.9 Age, Validity or Auxiliary Data Verification	28
7.10 Modular Enhanced Role Authentication (mERA)	28
Annex A (normative) Command set.....	29
A.1 CLASS byte coding.....	29
A.2 Command chaining mechanisms.....	29
A.3 Extended length mechanism	30
A.4 Logical channels.....	31
A.5 Short and extended length fields	31
A.6 Status words	31
A.7 Command set	32
Annex B (normative) Cryptographic Information Application	54
B.1 Description	54
B.2 CIA data organisation.....	63
Annex C (normative) Mandatory features	83
C.1 General.....	83
C.2 Data elements and data structures	83

C.3	Card services	84
C.4	Command set.....	84
C.5	Device Authentication and Key Derivation	85
C.6	Digital signature	85
C.7	Client/Server Authentication	86
C.8	Encryption Key Decipherment	86
Annex D (informative)	Optional features	87
D.1	General	87
D.2	Data elements and data structures.....	87
D.3	Card services	88
D.4	Command set.....	88
D.5	Device Authentication and Key Derivation	89
D.6	Digital signature	89
Annex E (informative)	Application Profiles	90
E.1	General	90
E.2	Application Profile 1: ICAO Application with EAC features.....	90
E.3	Application Profile 2: Travel Document Application	96
E.4	Application Profile 3: eID Application	101
E.5	Application Profile 4: Digital Signature Application	111
E.6	E.6 Application Profile 5: eServices Application using a trusted third party.....	121
E.7	Application Profile 6: Health Insurance Application.....	136
E.8	Application Profile 7: Combined eID and signature application	152
E.9	Application Profile 8: Multi-Service application	156
Annex F (informative)	Access rules in expanded format.....	161
F.1	Object protection by access rules in expanded format	161
F.2	Access rules in expanded format.....	161
F.3	Security attribute referencing expanded format	162
F.4	Security attribute template for physical interfaces.....	163
Annex G (informative)	Example of data structure: the Security Data Objects concept	164
G.1	SDO concept.....	164
Bibliography.....		176

Foreword

This document (CEN/TS 15480-2:2012) 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.

This document supersedes CEN/TS 15480-2:2007.

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

This Technical Specification specifies the logical characteristics and security features at the card/system interface for the European Citizen Card.

The European Citizen Card is a smart card with Identification, Authentication and electronic Signature (IAS) services. Therefore:

- 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 Technical Specification aims to ensure the interoperability at card/system interface in the usage phase.

In order to reach the interoperability objective, IAS services are compliant with EN 14890 Part 1 and Part 2. As the EN documents offer options, this specification fully defines a complete profile.

This Technical Specification also considers ICAO Doc 9303.

This Technical Specification does not mandate the use of a particular technology, and is intended to allow both native and Java card technologies.

This specification encompasses mandatory and optional features. Optional features make up a toolbox of modular options from which issuers can pick up the necessary protocols to fulfil the requirements for use. Mandatory features shall be implemented for a smart card to be compliant with this Technical Specification. Mandatory features required for compliancy to ECC specification are given in Annex C, the optional features are given in Annex D. Two IAS-enabled smart cards issued by two different issuers, and compliant with this Technical Specification but implementing different application profiles out of this Technical Specification, can interoperate with a terminal provided that such a terminal supports both application profiles. 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.

All the APDU commands described in this Technical Specification are in accordance with ISO/IEC 7816 Part 4 or Part 8. They are fully described here in order to provide the settings adopted by this specification and to prevent any ambiguity in case of several possible interpretations of the standards.

For physical, electrical and transport protocol characteristics, refer to CEN/TS 15480-1.

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.

EN 14890-1:2008:2008, *Application Interface for smart cards used as Secure Signature Creation Devices — Part 1: Basic requirements*

ISO/IEC 7816-3, *Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 3: Electronic signals and transmission protocols*

ISO/IEC 7816-4:2005, *Identification cards — Integrated circuit(s) cards — Part 4: Organisation, security and commands for interchange*

This is a free preview. Purchase the entire publication at the link below:

[Product Page](#)

-
- [Looking for additional Standards? Visit Intertek Inform Infostore](#)
 - [Learn about LexConnect, All Jurisdictions, Standards referenced in Australian legislation](#)
-