TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN/TS 15480-2

April 2007

ICS 35.240.15

English Version

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

Systèmes des cartes d'identification - Carte Européenne du Citoyen - Partie 2: Structures logiques des données et services cartes

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

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.

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

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

Ref. No. CEN/TS 15480-2:2007: E

Contents

Page

Foreword

This document (CEN/TS 15480-2:2007) 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* consist of the two 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.

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 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 prEN 14890 part 1 and part 2. As the CWA documents offer options, this specification fully defines a complete profile. This specification also provides other features not defined in the CWA documents (biometric on card matching, command chaining, role authentication …).

This Technical Specification is also compliant with ICAO specification (authentication methods, basic access control …).

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 requisites of their use cases. Mandatory features are necessarily to be implemented for a smart card to be compliant to this Technical Specification. Two IAS-enabled smart cards issued by two different issuers, and compliant with this Technical Specification but implementing different modular options out of this Technical Specification, can interoperate with a terminal provided such a terminal supports both options. 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 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.

ANSI X9.63, *Public Key Cryptography For the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography, January 8th 1999*

prEN 14890-1:2007, *Application Interface for smart cards used as Secure Signature Creation Devices — Part 1: Basic requirements*

prEN 14890-2:2007, *Application Interface for smart cards used as Secure Signature Creation Devices — Part 2: Additional Services*

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

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

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

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

ISO/IEC 9796-2, *Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Integer factorisation based mechanisms*

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

ISO/IEC 15946-2, *Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 2: Digital signatures*

ISO/IEC 19794-2, *Information technology — Biometric data interchange formats — Part 2: Finger minutiae data*

3 Terms and definitions

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

3.1
Application Dedicated File (ADF)
ADF is a Dedicated File (DF) with an Application Identifier (AID)

3.2
root
Master File MF in case of a native operating system, the applet instance having the default selection privilege in case of a Java card implementation

4 Abbreviations

4.1 Abbreviations

ADF Application Dedicated File

AID Application Identifier

AMB Access Mode Byte

AT Authentication Template

ATR Answer to Reset

ATS Answer to Select