EESTI STANDARD EVS-EN 419212-1:2014

Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic services

EESTI STANDARDIKESKUS EVS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

See Eesti standard EVS-EN 419212-1:2014 sisaldab Euroopa standardi EN 419212-1:2014 ingliskeelset teksti.	This Estonian standard EVS-EN 419212-1:2014 consists of the English text of the European standard EN 419212-1:2014.
Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 10.12.2014.	Date of Availability of the European standard is 10.12.2014.
Standard on kättesaadav Eesti Standardikeskusest.	The standard is available from the Estonian Centre for Standardisation.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 35.240.15

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 419212-1

December 2014

ICS 35.240.15

Supersedes EN 14890-1:2008

English Version

Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic services

Interface applicative des cartes à puces utilisées comme dispositifs de création de signature numérique sécurisés - Partie 1 : Services de base

Anwendungsschnittstelle für Chip-Karten, die zur Erzeugung qualifizierter elektronischer Signaturen verwendet werden - Teil 1: Allgemeine Dienste

This European Standard was approved by CEN on 27 September 2014.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

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

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. EN 419212-1:2014 E

Contents

Foreword

This document (EN 419212-1:2014) 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.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by June 2015 and conflicting national standards shall be withdrawn at the latest by June 2015.

This document supersedes EN 14890-1:2008.

This document has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association.

EN 419212, *Application Interface for smart cards used as Secure Signature Creation Devices*, consists of two parts:

- *Part 1: Basic services*;[the present document] which describes the specifications for IAS based services on smart cards to be used in compliance to the requirements of Article 5.1 of the Electronic Signature Directive; and

- *Part 2: Additional services* which describes other services that may be used in conjunction with all, some or none of the services described in Part 1.

This standard supports services in the context of **I**dentification, **A**uthentication and Electronic **S**ignature (IAS) services, as well as other services.

In this Part 1 of EN 419212, the standard allows support of implementations of the European legal framework for electronic signatures, defining the functional and security features for a smart card intended to be used as a Secure Signature Creation Device according to the Terms of the European Directive on Electronic Signature 1999/93/EC. A card compliant to the standard will be able to produce a "Qualified electronic signature" that fulfils the requirements of Article 5.1 of the Electronic Signature Directive and therefore can be considered equivalent to a hand-written signature.

EN 419212-2 specifies mechanisms to support other services like generic identification, authentication, confidentiality and signature verification services.

EN 419212 defines a set of services that will enable the development of interoperable cards issued by any card industry sector. The standard describes an application interface and behavior of the SSCD, i.e. it should be possible to implement it on native and interpreter based cards.

Compared with the 2008 versions of EN 14890, the following broad change has been made:

The scope of the standard was enhanced through new mechanisms in the field of password based mechanisms and privacy.

Regarding EN 419212-1, the most significant technical changes that have been made are the following ones:

- new algorithms added to device authentication protocols (e.g. AES, ELC);
- added AES to secure messaging;
- introduced password based mechanisms (PACEv2);
- updating references to their latest releases;

- algorithm Identifier coding;
- recommendation for making best use of device authentication protocols.

Regarding EN 419212-2, the most significant technical changes that have been made are the following ones:

a) added privacy services including:

   1) anonymity and pseudonymity services;

   2) auxiliary data transmission e.g. for Age verification;

   3) e-Services with trusted third party;

   4) e-Services with 2-parties.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: 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

The European Committee for Standardization (CEN)] draws attention to the fact that it is claimed that compliance with this document may involve the use of a patent concerning the mapping function given in 9.3.6 "Step 4.2 — Map nonce and compute generator point for integrated mapping".

The patent relates to "Sagem, MorphoMapping Patents FR09-54043 and FR09-54053, 2009".

CEN takes no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has assured CEN that he/she is willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with CEN. Information may be obtained from:

Morpho

11, boulevard Galliéni

92445 Issy-les-Moulineaux Cedex - France

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those identified above. CEN shall not be held responsible for identifying any or all such patent rights.”

1 Scope

This European Standard specifies mechanisms for smart cards to be used as secure signature creation devices covering:

- signature creation;
- user verification;
- password based authentication;
- device authentication;
- establishment of a secure channel.

The specified mechanisms are suitable for other purposes like services in the context of IAS.

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 419212-2:2014, *Application Interface for smart cards used as Secure Signature Creation Devices — Part 2: Additional services*

ISO 3166 (all parts), *Codes for the representation of names of countries and their subdivisions*

ISO 11568-2, *Financial services — Key management (retail) — Part 2: Symmetric ciphers, their key management and life cycle*

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

ISO/IEC 7816-4:2013, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*

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

ISO/IEC 7816-8:2004, *Identification cards — Integrated circuit cards — Part 8: Commands for security operations*

ISO/IEC 7816-11:2004, *Identification cards — Integrated circuit cards — Part 11: Personal verification through biometric methods*

ISO/IEC 7816-15:2004, *Identification cards — Integrated circuit cards — Part 15: Cryptographic information application*

ISO/IEC 8859 (all parts), *Information technology — 8-bit single-byte coded graphic character sets*

ISO/IEC 9796 (all parts), *Information technology — Security techniques — Digital signature schemes giving message recovery*

ISO/IEC 9797-1, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*

ISO/IEC 14888-2, *Information technology — Security techniques — Digital signatures with appendix — Part 2, Integer factorization based mechanisms*

ISO/IEC 14888-3, *Information technology — Security techniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms*

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.

NOTE These definitions are in compliance with those given in the revision of ISO/IEC 7816-4.

3.1
anonymity
assurance that a user may use a resource or service without disclosing their user identity

3.2
anonymization
process that removes the association between an identifying data set and a data subject

3.3
anonymized data
data that was once linked to an individual but can now no longer be related to them

3.4
anonymous data
data that cannot be linked to a specific individual

3.5
answer-to-Reset file
elementary file which indicates operating characteristics of the card

3.6
a priori trusted
operating environment which by definition can be trusted without further device authentication

EXAMPLE An example of this is the use within a company, where any available access point is connected to a trusted network.

3.7
authentication
verification that an entity is the claimed one [56]

3.8
command-response pair
set of two messages: a command followed by a response

3.9
confidentiality protection
prevention of information disclosure to unauthorized individuals, entities or systems [56]

3.10
data unit
smallest set of bits which can be unambiguously referenced

3.11
data element
item of information seen at the interface for which are defined a name, a description of logical content, a format and a coding