NSAI
Standards

Irish Standard
I.S. EN 419212-1:2017

Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part 1: Introduction and common definitions

I.S. EN 419212-1:2017

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/revises/consolidates the NSAI adoption of the document(s) indicated on the CEN/CENELEC cover/Foreword and the following National document(s):

NOTE: The date of any NSAI previous adoption may not match the date of its original CEN/CENELEC document.

This document is based on:	*Published:*
EN 419212-1:2017	2017-09-20

This document was published under the authority of the NSAI and comes into effect on: 2017-10-09	ICS number: 35.240.15 NOTE: If blank see CEN/CENELEC cover page

National Foreword

I.S. EN 419212-1:2017 is the adopted Irish version of the European Document EN 419212-1:2017, Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part 1: Introduction and common definitions

This document does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

For relationships with other publications refer to the NSAI web store.

Compliance with this document does not of itself confer immunity from legal obligations.

In line with international standards practice the decimal point is shown as a comma (,) throughout this document.

This page is intentionally left blank

I.S. EN 419212-1:2017

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 419212-1

September 2017

ICS 35.240.15

Supersedes EN 419212-1:2014, EN 419212-2:2014

English Version

Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part 1: Introduction and common definitions

Interface applicative des éléments sécurisés utilisés comme dispositifs de création de signature électronique qualifiée (cachet) - Partie 1 : Introduction et définitions communes

Anwendungsschnittstelle für sichere Elemente, die als qualifizierte elektronischer Signatur- /Siegelerstellungseinheiten verwendet werden - Teil 1: Allgemeine Dienste

This European Standard was approved by CEN on 6 February 2017.

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, Serbia, 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 419212-1:2017 E

EN 419212-1:2017 (E)

Contents

This is a free page sample. Access the full version online.
I.S. EN 419212-1:2017

EN 419212-1:2017 (E)

This is a free page sample. Access the full version online.
I.S. EN 419212-1:2017

EN 419212-1:2017 (E)

European foreword

This document (EN 419212-1:2017) has been prepared by Technical Committee CEN/TC 224 "Furniture", 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 March 2018, and conflicting national standards shall be withdrawn at the latest by March 2018.

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

This document supersedes EN 419212-1:2014 and EN 419212-2:2014.

This standard supports services in the context of **e**lectronic **ID**entification, **A**uthentication and Trust **S**ervices (eIDAS) including signatures.

In EN 419212-2, the standard allows support of implementations of the European legal framework for electronic signatures, defining the functional and security features for a Secure Elements (SE) (e.g. smart cards) intended to be used as a Qualified electronic Signature Creation Device (QSCD) according to the Terms of the "European Regulation on Electronic Identification and Trust Services for electronic transactions in the internal market" [2].

A Secure Element (SE) compliant to the standard will be able to produce a "qualified electronic signature" that fulfils the requirements of Article of the Electronic Signature Regulation and therefore can be considered equivalent to a hand-written signature [2].

This standard consists of five parts:

Part 1: "Introduction and common definitions" describes the history, application context, market perspective and a tutorial about the basic understanding of electronic signatures. It also provides common terms and references valid for the entire 419212 series.

Part 2: "Signature and Seal Services" describes the specifications for signature generation according to the eIDAS regulation.

Part 3: "Device Authentication" describes the device authentication protocols and the related key management services to establish a secure channel.

Part 4: "Privacy specific Protocols" describes functions and services to provide privacy to identification services.

Part 5: "Trusted eServices" describes services that may be used in conjunction with signature services described in Part 2.

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

According to the CEN-CENELEC Internal Regulations, the national standards organisations 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, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

EN 419212-1:2017 (E)

Introduction

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

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 EN 419212-2, clause 8.3.6 "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 ensured 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

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 part is an informative introduction into the following parts. It gives guidance to the following parts in order to allow an efficient usage of the provided information. Therefore Part 1 provides history, application context, market perspective and a tutorial about the basic understanding of electronic signatures.

- Clause 3 provides "Terms and definitions" covering all parts of this standards. The specific parts will contain a similar section which refers to the clause of this Part 1.

- Clause 4 provides "Symbols and abbreviations" covering all parts of this standards. The specific parts will contain a similar section which refers to the clause of this Part 1.

- Clause 5 provides a Management Summary that describes the market context in which electronic signatures are typically

- Annex A provides the algorithm identifies for all parts of the standard.

- Annex B provides the algorithm identifies for all parts of the standard.

- Annex C provides the build scheme for object identifiers for all parts of the standard.

- Annex D "Tutorial on Signature Technology" provides a tutorial which helps the first reader to get familiar with signature technology and its relation to the society that it serves.

- Annex E "Guide to the EN 419212" explains the historical and technical evolution of the ESIGN activities which did finally lead to this version of the signature standard.

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.

ISO/IEC 7816-3:2006, *Identification cards — Integrated circuit cards — Part 3: Cards with contacts — Electrical interface and transmission protocols*

ISO/IEC 9796-2:2010, *Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms*

ISO 7498-2, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture*

3 Terms and definitions

For the purposes of Part 1 to 5 of this series of standards, 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
advanced electronic seal
electronic seal which meets the following requirements:

a) it is uniquely linked to the creator of the seal;

b) it is capable of identifying the creator of the seal;

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

Product Page