ICS 35.240.15 SLOVENSKÁ TECHNICKÁ NORMA Jún 2018

STN	**Aplikačné rozhranie pre bezpečné prvky na elektronickú identifikáciu, autentifikáciu a dôveryhodné služby** **Časť 2: Podpisy a služby pečiatok**	**STN** **EN 419212-2** 36 9724

Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part 2: Signature and Seal Services

Táto norma obsahuje anglickú verziu európskej normy.
This standard includes the English version of the European Standard.

Táto norma bola oznámená vo Vestníku ÚNMS SR č. 05/18

Obsahuje: EN 419212-2:2017

Spolu s STN EN 419212-1 a STN EN 419212-3 ruší
STN EN 419212-1 (36 9724) z júna 2015

STN EN 419212-2 (36 9724) z júna 2015

EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN 419212-2

December 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 2: Signature and Seal Services

Interface applicative des éléments sécurisés utilisés comme dispositifs de création de signature électronique qualifiée (cachet) - Partie 2 : Services de signatures et de cachets

Anwendungsschnittstelle für sichere Elemente, die als qualifizierte elektronische Signatur-/Siegelerstellungseinheiten verwendet werden - Teil 2: Zusätzliche Dienste

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

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

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

Contents

Page

European foreword

This document (EN 419212-2:2017) 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of an identical text or by endorsement, at the latest by June 2018, and conflicting national standards shall be withdrawn at the latest by June 2018.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 Part 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 " [2] and therefore can be considered equivalent to a hand-written signature.

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.

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 Part 2, clause 8.3.6.

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 specifies mechanisms for SEs to be used as qualified signature creation devices covering

- Signature creation and mobile signature creation
- User verification
- Password based authentication

The specified mechanisms are suitable for other purposes like services in the context of [2].

The particular case of seal is also covered by the specification. The differences between seal and signature is exposed in Annex B. Annex B also explains how the mechanisms for SEs as qualified signature creation devices can be used for SEs as qualified seal creation devices.

Mobile signature is an alternative to the classical signature case which is performed by a secure element. Mobile signature is encouraged by the large widespread of mobile devices and the qualification authorized by the eIDAS Regulation [2]. The particular case of remote signature (or server signing) is covered by this specification in Annex C.

In the rest of this document, except Annex B, there will be no particular notion of a seal since it technically compares to the signature.

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 7816-4:2013, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands 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, *Identification cards — Integrated circuit cards — Part 15: Cryptographic information application*

ISO/IEC 9797-1:2011, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*

ISO 11568-2:2012, *Financial services — Key management (retail) — Part 2: Symmetric ciphers, their key management and life cycle*

ISO/IEC 14888-2:2008, *Information technology — Security techniques — Digital signatures with appendix — Part 2: Integer factorization based mechanisms*

ISO/IEC 19794-2:2005, *Information technology — Biometric data interchange formats — Part 2: Finger minutiae data*

ISO/IEC 15946-5, *Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 5: Elliptic curve generation, 2009-12-15*

BSI: "Technical report Signature creation and administration for eIDAS token", Part 1: Functional Specification Version 1.0 Date: 2015/07/21

BSI/TR-03110 "Part 2 – Protocols for electronic IDentification, Authentication and trust Services (eIDAS)", Version 2.20, January 22nd, 2015[1]

[1] Available at https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03110/index_htm.html