ICS 35.240.15 SLOVENSKÁ TECHNICKÁ NORMA Október 2018

STN	**Aplikačné rozhranie pre bezpečné prvky na elektronickú identifikáciu, autentifikáciu a dôveryhodné služby Časť 4: Protokoly špecifické pre ochranu osobných údajov**	**STN EN 419212-4 36 9721**

Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part 4: Privacy specific Protocols

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. 09/18

Obsahuje: EN 419212-4:2018

Spolu s STN EN 419212-1, STN EN 419212-3, STN EN 419212-2 a STN EN 419212-5 ruší
STN EN 419212-1 (36 9724) z júna 2015

STN EN 419212-2 (36 9724) z júna 2015

127348

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 419212-4

April 2018

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 4: Privacy specific Protocols

Interface applicative des éléments sécurisés pour les services électroniques d'identification, d'authentification et de confiance - Partie 4 : Protocoles spécifiques à la protection de la vie privée

Anwendungsschnittstelle für sichere Elemente zur elektronischen Identifikation, Authentisierung und für vertrauenswürdige Dienste - Teil 4: Datenschutzspezifische Protokolle

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: Rue de la Science 23, B-1040 Brussels

Ref. No. EN 419212-4:2018 E

Contents

Page

European foreword

This document (EN 419212-4:2018) has been prepared by Technical Committee CEN/TC 224 “Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment”, 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 October 2018, and conflicting national standards shall be withdrawn at the latest by October 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 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”.

A Secure Element (SE) compliant to the standard will be able to produce a “qualified electronic signature” that fulfils the requirements of section 4, in particular Articles 26 (requirements for advanced electronic signatures) and 29 (requirements for qualified electronic signature creation devices) of the so-called eIDAS Regulation 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.

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 EN 419212-2:2017 8.2.

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 privacy-enabled devices in the context of IAS, and fulfill the requirements of Article 5 of the so-called eIDAS Regulation about data processing and protection.

It covers:

- Age verification
- Document validation
- Restricted identification
- eServices with trusted third party based on ERA protocol

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 7816-8:2016, *Integrated circuit(s) cards with contacts — Part 8: Commands and mechanisms for security operations*

Technical Guideline TR-03110 2.20, “Advanced Security Mechanisms for Machine Readable Travel Documents - Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE) and Restricted Identification (RI) Version 2.20 Beta”,, Privacy Context functions