ICS 35.240.15 SLOVENSKÁ TECHNICKÁ NORMA Jún 2015

STN	**Aplikačné rozhranie pre smart karty používané ako bezpečné zariadenia na vyhotovenie podpisu. Časť 2: Dodatočné služby.**	**STN EN 419212-2** 36 9724

Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional 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. 05/15

Obsahuje: EN 419212-2:2014

Oznámením tejto normy sa ruší
STN EN 14890-2 (36 9724) z júna 2009

120736

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 419212-2

December 2014

ICS 35.240.15

Supersedes EN 14890-2:2008

English Version

Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional services

Interface applicative des cartes à puces utilisées comme dispositifs de création de signature numérique sécurisés - Partie 2 : Services complémentaires

Anwendungsschnittstelle für Chip-Karten, die zur Erzeugung qualifizierter elektronischer Signaturen verwendet werden - Teil 2: Zusätzliche 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 419212-2:2014 E

Contents

Foreword

This document (EN 419212-2:2014) 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.

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

This document supersedes EN 14890-2:2008.

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* 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* [the present document] 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 IAS **I**dentification, **A**uthentication and Electronic **S**ignature (IAS) services, as well as other services.

In EN 419212-1, the standard allows to support the implementation 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 (QES)" that fulfils the requirements of Article 5.1 of the Electronic Signature Directive and therefore can be considered equivalent to hand-written signatures.

In EN 419212-2, the standard specifies mechanisms to support other services like generic Identification, Authentication, confidentiality, signature verification services and privacy features.

EN 419212 defines a set of services that will enable the development of interoperable cards issued by any card industry sector. The standard will describe 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.

1 Scope

This European Standard contains Identification, Authentication and Digital Signature (IAS) services in addition to the SSCD mechanisms already described in EN 419212-1 to enable interoperability and usage for IAS services on a national or European level.

It also specifies additional mechanisms like key decipherment, Client Server authentication, identity management and privacy related services.

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 419212-1:2014, *Application Interface for smart cards used as Secure Signature Creation Devices — Part 1: Basic services*

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

ISO/IEC 7816-6:2006, *Identification cards — Integrated circuit(s) cards with contacts — Part 6: Interindustry data elements for interchange*

ISO/IEC 7816-8:2004, *Integrated circuit(s) cards with contacts — Part 8: Commands for security operations*

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*