ICS 03.160, 35.040, 35.240.15 SLOVENSKÁ TECHNICKÁ NORMA Apríl 2014

STN	**Profily ochrany pre zariadenia na vyhotovenie bezpečného podpisu. Časť 4: Rozšírenie pre zariadenie s generovaním kľúča a dôveryhodným kanálom k aplikácii na generovanie certifikátov.**	**STN EN 419211-4** 97 6001

Protection profiles for secure signature creation device - Part 4: Extension for device with key generation and trusted channel to certificate generation application

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

Obsahuje: EN 419211-4:2013

118798

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 419211-4

November 2013

ICS 03.160; 35.040; 35.240.15

Supersedes CWA 14169:2004

English Version

Protection profiles for secure signature creation device - Part 4: Extension for device with key generation and trusted channel to certificate generation application

Profils de protection pour dispositif sécurisé de création de signature électronique - Partie 4: Extension pour un dispositif avec génération de clé et communication sécurisée avec l'application de génération de certificats

Schutzprofile für sichere Signaturerstellungseinheiten - Teil 4: Erweiterung für Einheiten mit Schlüsselerzeugung und vertrauenswürdigem Kanal zur Zertifikaterzeugungsanwendung

This European Standard was approved by CEN on 12 October 2013.

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

Contents

Page

Foreword

This document (EN 419211-4:2013) 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 May 2014 and conflicting national standards shall be withdrawn at the latest by May 2014.

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 CWA 14169:2004.

This series of European Standards, *Protection profiles for secure signature creation device* consists of the following parts:

— *Part 1: Overview*

— *Part 2: Device with key generation*

— *Part 3: Device with key import*

— *Part 4: Extension for device with key generation and trusted channel to certificate generation application*

— *Part 5: Extension for device with key generation and trusted channel to signature creation application*

— *Part 6: Extension for device with key import and trusted channel to signature creation application*

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

This series of European Standards specifies Common Criteria protection profiles for secure signature creation devices and is issued by the European Committee for Standardization, Information Society Standardization System (CEN/ISSS) as update of the Electronic Signatures (E-SIGN) CEN/ISSS workshop agreement (CWA) 14169:2004, Annex B and Annex C on the protection profile secure signature creation devices, “EAL 4+”.

Preparation of this document as a protection profile (PP) follows the rules of the Common Criteria version 3.1 [2], [3] and [4].

1 Scope

This European Standard specifies a protection profile for a secure signature creation device that may generate signing keys internally and export the public key in protected manner: secure signature creation device with key generation and trusted communication with certificate generation application (SSCD KG TCCGA).

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.

prEN 419211-1:2011, *Protection profiles for secure signature creation device — Part 1: Overview*[1)]

1) To be published. This document was submitted to the Enquiry procedure under reference prEN 14169-1.