

<b>STN</b>	<b>Profily ochrany pre zariadenia na vyhotovenie bezpečného podpisu. Časť 6: Rozšírenie pre zariadenie s importovaním kľúča a dôveryhodným kanálom k aplikácii na vyhotovenie podpisu.</b>	<b>STN EN 419211-6</b>  97 6001
------------	--	---

Protection profiles for secure signature creation device - Part 6: Extension for device with key import and trusted channel to signature creation application

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. 01/15

Obsahuje: EN 419211-6:2014

**120187**

---

Úrad pre normalizáciu, metrológiu a skúšobníctvo SR, odbor SÚTN, 2015  
Podľa zákona č. 264/1999 Z. z. v znení neskorších predpisov sa môžu slovenské technické normy rozmnožovať a rozširovať iba so súhlasom Úradu pre normalizáciu, metrológiu a skúšobníctvo SR.

English Version

## Protection profiles for secure signature creation device - Part 6: Extension for device with key import and trusted channel to signature creation application

Profils de protection pour dispositif sécurisé de création de signature électronique - Partie 6: Extension pour un dispositif avec import de clé et communication sécurisée avec l'application de création de signature

Schutzprofile für sichere Signaturerstellungseinheiten - Teil 6: Erweiterung für Einheiten mit Schlüsselimport und vertrauenswürdigen Kanal zur Signaturerstellungsanwendung

This European Standard was approved by CEN on 25 July 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**

<b>Contents</b>	<b>Page</b>
Foreword .....	3
Introduction .....	4
1 Scope .....	5
2 Normative references .....	5
3 Conventions and terminology .....	5
3.1 Conventions .....	5
3.2 Terms and definitions .....	5
4 PP introduction .....	6
4.1 PP reference .....	6
4.2 PP overview .....	6
4.3 TOE overview .....	7
5 Conformance claims .....	9
5.1 CC conformance claim .....	9
5.2 PP claim, Package claim .....	9
5.3 Conformance rationale .....	9
5.4 Conformance statement .....	10
6 Security problem definition .....	10
6.1 Assets, users and threat agents .....	10
6.2 Threats .....	11
6.3 Organizational security policies .....	11
6.4 Assumptions .....	11
7 Security objectives .....	11
7.1 Security objectives for the TOE .....	11
7.2 Security objectives for the operational environment .....	12
7.3 Security objectives rationale .....	12
8 Extended components definition .....	15
9 Security requirements .....	15
9.1 Security functional requirements .....	15
9.2 Security assurance requirements .....	18
9.3 Security requirements rationale .....	19
Bibliography .....	24

## Foreword

This document (EN 419211-6:2014) 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 April 2015 and conflicting national standards shall be withdrawn at the latest by April 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 CWA 14169:2004.

In comparison with CWA 14169, the entire document has been revised. Refer to EN 419211-1:2014, Annex A for more details.

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 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 (CEN) as an update of the Electronic Signatures (E-SIGN) CEN workshop agreement, CWA 14169:2004, Annex B and Annex C on the protection profile secure signature creation devices, "EAL 4+".

This series of European Standards 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*

Preparation of this document as a protection profile (PP) follows the rules of ISO/IEC 15408.

## 1 Scope

This European Standard specifies a protection profile for a secure signature creation device that may import signing keys and communicate with the signature creation application in protected manner: secure signature creation device with key import and trusted communication with signature creation application (SSCD KI TCSCA).

## 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 419211-1:2014, *Protection profiles for secure signature creation device — Part 1: Overview*

ISO/IEC 15408-1, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*<sup>1)</sup>

ISO/IEC 15408-2, *Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components*

ISO/IEC 15408-3, *Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components*

**koniec náhľadu – text ďalej pokračuje v platenej verzii STN**

---

<sup>1)</sup> ISO/IEC 15408-1, ISO/IEC 15408-2 and ISO/IEC 15408-3 respectively correspond to *Common Criteria for Information Technology Security Evaluation*, Parts 1, 2 and 3.