

STN	Profily ochrany pre zariadenia na vyhotovenie bezpečného podpisu. Časť 2: Zariadenie s generovaním kľúča.	STN EN 419211-2 97 6001
------------	--	---

Protection profiles for secure signature creation device - Part 2: Device with key generation

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. 12/13

Obsahuje: EN 419211-2:2013

English Version

Protection profiles for secure signature creation device - Part 2: Device with key generation

Profils de protection des dispositifs sécurisés de création
de signature - Partie 2: Dispositif avec génération de clé

Schutzprofile für sichere Signaturerstellungseinheiten - Teil
2: Geräte mit Schlüsselerzeugung

This European Standard was approved by CEN on 8 May 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

Management Centre: Avenue Marnix 17, B-1000 Brussels

Contents

Page

Foreword.....	3
1 Scope	4
2 Normative references	4
3 Conventions and terminology	4
4 PP introduction	4
5 Conformance claims	11
6 Security problem definition	11
7 Security objectives	13
8 Extended components definition	20
9 Security requirements	21
Bibliography	42

Foreword

This document (EN 419211-2:2013) 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 January 2014, and conflicting national standards shall be withdrawn at the latest by January 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 document was submitted to the Enquiry procedure under reference prEN 14169-2.

The EN 419211 series 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.

Correspondence and comments regarding this protection profile about secure signature creation device with key generation (PP SSCD KG) can be referred to the CEN/TC 224 Secretary.

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, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

1 Scope

This European Standard specifies a protection profile for a secure signature creation device that may generate signing keys internally: secure signature creation device with key generation (SSCD KG).

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, *Protection profiles for secure signature creation device — Part 1: Overview*¹⁾

ISO/IEC 15408-1:2009²⁾ *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC 15408-2²⁾, *Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components*

ISO/IEC 15408-3²⁾, *Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components*

koniec náhľadu – text ďalej pokračuje v platenej verzii STN