

STN	Ochranný profil pre zariadenie na vytvorenie bezpečného podpisu. Časť 3: Zariadenie s importovaním kľúča.	STN EN 419211-3 97 6001
------------	--	---

Protection profiles for secure signature creation device - Part 3: Device with key import

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

Obsahuje: EN 419211-3:2013

119132

Úrad pre normalizáciu, metrológiu a skúšobníctvo SR, odbor SÚTN, 2014
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 3:
Device with key import**Profils de protection des dispositifs sécurisés de création de
signature - Partie 3: Dispositif avec import de cléSchutzprofile für sichere Signaturerstellungseinheiten - Teil
3: Einheiten mit Schlüsselimport

This European Standard was approved by CEN on 14 September 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**

EN 419211-3:2013 (E)**Contents**

Foreword	3
1 Scope	5
2 Normative references	5
3 Terms and definitions	5
4 PP introduction	5
4.1 PP reference	5
4.2 PP overview	5
4.3 TOE overview	6
5 Conformance claims	11
5.1 CC conformance claim	11
5.2 PP claim, Package claim	11
5.3 Conformance rationale	11
5.4 Conformance statement	11
6 Security problem definition	12
6.1 Assets, users and threat agents	12
6.2 Threats	12
6.3 Organisational security policies	13
6.4 Assumptions	14
7 Security objectives	14
7.1 Security objectives for the TOE	14
7.2 Security objectives for the operational environment	16
7.3 Security objectives rationale	18
8 Extended components definition	22
9 Security requirements	23
9.1 Security functional requirements	23
9.2 Security assurance requirements	38
9.3 Security requirements rationale	39
Bibliography	45

Foreword

This document (EN 419211-3:2013) 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 April 2014, and conflicting national standards shall be withdrawn at the latest by April 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 CEN Enquiry under reference prEN 14169-3.

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.

EN 419211-3:2013 (E)**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+".

This series of European Standards consists of the following parts:

- *Protection profiles for secure signature creation device — Part 1: Overview;*
- *Protection profiles for secure signature creation device — Part 2: Device with key generation;*
- *Protection profiles for secure signature creation device — Part 3: Device with key import;*
- *Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted channel to certificate generation application;*
- *Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted channel to signature creation application;*
- *Protection profiles for secure signature creation device — 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 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 with signing keys import possibility: SSCD with key import (SSCD KI).

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 14169-1:2011, *Protection profiles for secure signature creation device — Part 1: Overview*

koniec náhľadu – text ďalej pokračuje v platenej verzii STN

¹ This European Directive is referred to in this PP as “the directive”.