Turvalise allkirja andmise vahendi kaitseprofiil. Osa 2: Võtme genereerimisega vahend

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

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

See Eesti standard EVS-EN 419211-2:2013 sisaldab Euroopa standardi EN 419211-2:2013 ingliskeelset teksti.	This Estonian standard EVS-EN 419211-2:2013 consists of the English text of the European standard EN 419211-2:2013.
Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas.	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 17.07.2013.	Date of Availability of the European standard is 17.07.2013.
Standard on kättesaadav Eesti Standardikeskusest.	The standard is available from the Estonian Centre for Standardisation.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 03.160, 35.040, 35.240.15

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 419211-2

July 2013

ICS 03.160; 35.040; 35.240.15

Supersedes CWA 14169:2004

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

Ref. No. EN 419211-2:2013: E

Contents

Page

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 15408-1:2009[2)] *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

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

ISO/IEC 15408-3[2)], *Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components*

3 Conventions and terminology

3.1 Conventions

The content and structure of this document follow the rules and conventions laid out in ISO/IEC 15408-1.

Normative aspects of content in this European Standard are specified according to the Common Criteria rules and not specifically identified by “shall”.

3.2 Terms and definitions

For the purposes of this document, the acronyms, terms and definitions given in prEN 419211-1 apply.

4 PP introduction

4.1 PP reference

Title:	Protection profiles for secure signature creation device — Part 2: Device with key generation
Version:	2.0.1.
Author:	CEN (TC224/WG17)
Publication date:	2013
Registration:	BSI-CC-PP-0059-2009-MA-01
CC version:	3.1 Revision 3

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

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