Turvalise allkirja andmise vahendi kaitseprofiil. Osa 5: Võtme genereerimisega vahendi ja usaldatava kanali laiendus allkirja andmise rakendusele

Protection profiles for secure signature creation device - Part 5: Extension for device with key generation and trusted channel to signature creation application

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

See Eesti standard EVS-EN 419211-5:2013 sisaldab Euroopa standardi EN 419211-5:2013 ingliskeelset teksti.	This Estonian standard EVS-EN 419211-5:2013 consists of the English text of the European standard EN 419211-5:2013.
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 04.12.2013.	Date of Availability of the European standard is 04.12.2013.
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 419211-5

December 2013

ICS 03.160; 35.040; 35.240.15

Supersedes CWA 14169:2004

English Version

Protection profiles for secure signature creation device - Part 5: Extension for device with key generation and trusted channel to signature creation application

Profils de protection pour dispositif sécurisé de création de signature - Partie 5: Extension pour un dispositif avec génération de clé et communication sécurisée avec l'application de création de signature

Schutzprofile für Sichere Signaturerstellungseinheiten - Teil 5: Erweiterung für Einheiten mit Schlüsselerzeugung und vertrauenswürdigem Kanal zur Signaturerstellungsanwendung

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

Ref. No. EN 419211-5:2013 E

Contents

Page

Foreword

This document (EN 419211-5:2013) 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 June 2014, and conflicting national standards shall be withdrawn at the latest by June 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 communicate with the signature creation application in protected manner: secure signature creation device with key generation and trusted communication with signature creation application (SSCD KG 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.

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

3 Conventions and terminology

3.1 Conventions

This document is drafted in accordance with the CEN-CENELEC Internal Regulations Part 3 and content and structure of this document follow the rules and conventions laid out in Common Criteria 3.1.

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

3.2 Terms and definitions

For the purposes of this document, the acronyms, terms and definitions given in prEN 419211-1:2011 apply.

4 PP introduction

4.1 PP reference

Title:	Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted communication with signature creation application
Version:	1.0.1
Author:	CEN / CENELEC (TC224/WG17)
Publication date:	2012–11–14
Registration:	BSI-CC-PP-0072
CC version:	3.1 Revision 4
Editor:	Arnold Abromeit, TÜV Informationstechnik GmbH
General status:	final
Keywords:	secure signature creation device, electronic signature, digital signature, key generation, trusted communication with signature creation application

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