Turvalise allkirja andmise vahendi kaitseprofiil. Osa 1: Ülevaade

Protection profiles for secure signature creation device - Part 1: Overview

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

See Eesti standard EVS-EN 419211-1:2014 sisaldab Euroopa standardi EN 419211-1:2014 inglisekeelset teksti.	This Estonian standard EVS-EN 419211-1:2014 consists of the English text of the European standard EN 419211-1:2014.
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 08.10.2014.	Date of Availability of the European standard is 08.10.2014.
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 35.240.15

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 419211-1

October 2014

ICS 35.240.15

Supersedes CWA 14169:2004

English Version

Protection profiles for secure signature creation device - Part 1: Overview

Profils de protection pour dispositif sécurisé de création de signature électronique - Partie 1: Présentation générale

Schutzprofile für sichere Signaturerstellungseinheiten - Teil 1: Überblick

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

Ref. No. EN 419211-1:2014 E

Contents

Page

Foreword

This document (EN 419211-1:2014) 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.

Significant changes between this edition and CWA 14169:2004 can be found in Annex A.

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 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 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 communication with certificate generation application*

— *Part 5: Extension for device with key generation and trusted communication with signature creation application*

— *Part 6: Extension for device with key import and trusted communication with signature creation application*

Preparation of the documents in this series of European Standards as protection profiles follows the rules of the Common Criteria version 3.1 ([2], [3] and [4]).

1 Scope

This European Standard:

— specifies terms used in specifying protection profiles for secure signature creation devices,

— specifies functional and operational requirements for secure signature creation devices,

— describes the targets of evaluation for these protection profiles.

2 Normative references

Not applicable.

3 Terminology

For the purposes of this document, the following terms and definitions apply.

3.1 Legislative references

This European Standard reflects the requirement of a European Directive in the technical terms of a protection profile. The following terms are used in the text to reference this Directive:

3.1.1
the Directive
Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on "*a Community framework for electronic signatures"* [1]

Note 1 to entry: References in this document to a specific article and paragraph of Directive 1999/93/EC are of the form "(**the Directive:** n.m)".

3.1.2
annex
one of the annexes, Annex I, Annex II or Annex III of **the Directive**

3.2 Technical terms

3.2.1
administrator
user who performs TOE initialization, TOE personalization, or other TOE administrative functions

3.2.2
advanced electronic signature
digital signature which meets specific requirements in **the Directive: 2.2**

Note 1 to entry: According to **the Directive** a digital signature qualifies as an advanced electronic signature if it:

— is uniquely linked to the signatory;

— is capable of identifying the signatory;

— is created using means that the signatory can maintain under their sole control; and

— is linked to the data to which it relates in such a manner that any subsequent change of the data are detectable.