

**Turvalise allkirja andmise vahendi kaitseprofiil. Osa 6:
Võtme impordiga vahendi ja usaldatava kanali laiendus
allkirja andmise rakendusele**

**Protection profiles for secure signature creation device -
Part 6: Extension for device with key import and trusted
channel to signature creation application**

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

See Eesti standard EVS-EN 419211-6:2014 sisaldab Euroopa standardi EN 419211-6:2014 inglisekeelset teksti.	This Estonian standard EVS-EN 419211-6:2014 consists of the English text of the European standard EN 419211-6:2014.
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 03.160, 35.040, 35.240.15

Standardite reprodutseerimise ja levitamise õigus kuulub Eesti Standardikeskusele

Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonsesse süsteemi või edastamine ükskõik millises vormis või millisel teel ilma Eesti Standardikeskuse kirjaliku loata on keelatud.

Kui Teil on küsimusi standardite autorikaitse kohta, võtke palun ühendust Eesti Standardikeskusega:
Aru 10, 10317 Tallinn, Eesti; www.evs.ee; telefon 605 5050; e-post info@evs.ee

The right to reproduce and distribute standards belongs to the Estonian Centre for Standardisation

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, without a written permission from the Estonian Centre for Standardisation.

If you have any questions about copyright, please contact Estonian Centre for Standardisation:
Aru 10, 10317 Tallinn, Estonia; www.evs.ee; phone 605 5050; e-mail info@evs.ee

English Version

Protection profiles for secure signature creation device - Part 6:
Extension for device with key import and trusted channel to
signature creation application

Profils de protection pour dispositif sécurisé de création de
signature électronique - Partie 6: Extension pour un
dispositif avec import de clé et communication sécurisée
avec l'application de création de signature

Schutzprofile für sichere Signaturerstellungseinheiten - Teil
6: Erweiterung für Einheiten mit Schlüsselimport und
vertrauenswürdigen Kanal zur
Signaturerstellungsanwendung

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

Contents

Page

Foreword	3
Introduction	4
1 Scope	5
2 Normative references	5
3 Conventions and terminology	5
3.1 Conventions	5
3.2 Terms and definitions	5
4 PP introduction	6
4.1 PP reference	6
4.2 PP overview	6
4.3 TOE overview	7
5 Conformance claims	9
5.1 CC conformance claim	9
5.2 PP claim, Package claim	9
5.3 Conformance rationale	9
5.4 Conformance statement	10
6 Security problem definition	10
6.1 Assets, users and threat agents	10
6.2 Threats	11
6.3 Organizational security policies	11
6.4 Assumptions	11
7 Security objectives	11
7.1 Security objectives for the TOE	11
7.2 Security objectives for the operational environment	12
7.3 Security objectives rationale	12
8 Extended components definition	15
9 Security requirements	15
9.1 Security functional requirements	15
9.2 Security assurance requirements	18
9.3 Security requirements rationale	19
Bibliography	24

Foreword

This document (EN 419211-6:2014) 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.

In comparison with CWA 14169, the entire document has been revised. Refer to EN 419211-1:2014, Annex A for more details.

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 Common Criteria 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 B and 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 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 Scope

This European Standard specifies a protection profile for a secure signature creation device that may import signing keys and communicate with the signature creation application in protected manner: secure signature creation device with key import and trusted communication with signature creation application (SSCD KI 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.

EN 419211-1:2014, *Protection profiles for secure signature creation device — Part 1: Overview*

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

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

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

3 Conventions and terminology

3.1 Conventions

This document is drafted in accordance with the CEN/CENELEC directive and content and structure of this document follow the rules and conventions laid out in ISO/IEC 15408.

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 EN 419211-1 apply.

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