

Protection profile for trustworthy systems supporting  
time stamping

## EESTI STANDARDI EESSÕNA

## NATIONAL FOREWORD

|                                                                                                                     |                                                                                                                                    |
|---------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| See Eesti standard EVS-EN 419231:2019 sisaldab Euroopa standardi EN 419231:2019 ingliskeelset teksti.               | This Estonian standard EVS-EN 419231:2019 consists of the English text of the European standard EN 419231:2019.                    |
| 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 29.08.2019. | Date of Availability of the European standard is 29.08.2019.                                                                       |
| 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](mailto:standardiosakond@evs.ee).

ICS 35.030, 35.040.01

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:  
Koduleht [www.evs.ee](http://www.evs.ee); telefon 605 5050; e-post [info@evs.ee](mailto: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:

Homepage [www.evs.ee](http://www.evs.ee); phone +372 605 5050; e-mail [info@evs.ee](mailto:info@evs.ee)

English Version

## Protection profile for trustworthy systems supporting time stamping

Profil de protection pour des systèmes fiables  
d'horodatage

Schutzprofil für vertrauenswürdige Systeme, die  
Zeitstempel unterstützen

This European Standard was approved by CEN on 7 July 2019.

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, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, 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: Rue de la Science 23, B-1040 Brussels

| <b>Contents</b>                                                 | <b>Page</b> |
|-----------------------------------------------------------------|-------------|
| <b>European foreword</b> .....                                  | <b>3</b>    |
| <b>Introduction</b> .....                                       | <b>4</b>    |
| <b>1 Scope</b> .....                                            | <b>5</b>    |
| <b>2 Normative references</b> .....                             | <b>5</b>    |
| <b>3 Terms, definitions and abbreviations</b> .....             | <b>5</b>    |
| 3.1 Terms and definitions .....                                 | 5           |
| 3.2 Abbreviations .....                                         | 11          |
| <b>4 Introduction</b> .....                                     | <b>12</b>   |
| 4.1 PP reference .....                                          | 12          |
| 4.2 TOE overview.....                                           | 12          |
| <b>5 Conformance claims</b> .....                               | <b>18</b>   |
| 5.1 CC conformance claim .....                                  | 18          |
| 5.2 PP claim .....                                              | 18          |
| 5.3 Conformance rationale .....                                 | 18          |
| 5.4 Conformance statement.....                                  | 18          |
| <b>6 Security problem definition</b> .....                      | <b>19</b>   |
| 6.1 TOE assets.....                                             | 19          |
| 6.2 Threats.....                                                | 21          |
| 6.3 Organizational security policies .....                      | 24          |
| 6.4 Assumptions.....                                            | 25          |
| <b>7 Security objectives</b> .....                              | <b>27</b>   |
| 7.1 General.....                                                | 27          |
| 7.2 Security objectives for the TOE.....                        | 27          |
| 7.3 Security objectives for the operational environment.....    | 29          |
| 7.4 Security objectives rationale .....                         | 31          |
| <b>8 Security functional requirements</b> .....                 | <b>37</b>   |
| 8.1 General.....                                                | 37          |
| 8.2 Subjects, objects, operations and security attributes ..... | 37          |
| 8.3 Security requirements operations.....                       | 40          |
| 8.4 User Data Protection (FDP) .....                            | 40          |
| 8.5 Security Management (FMT).....                              | 47          |
| 8.6 Protection of the TSF (FPT) .....                           | 50          |
| 8.7 Trusted Path/Channels (FTP).....                            | 50          |
| 8.8 Cryptographic Support (FCS) .....                           | 51          |
| 8.9 Identification and Authentication (FIA) .....               | 52          |
| 8.10 Security Audit (FAU) .....                                 | 52          |
| <b>9 Security assurance requirements</b> .....                  | <b>54</b>   |
| <b>10 Security requirements rationale</b> .....                 | <b>55</b>   |
| 10.1 Security functional requirements rationale.....            | 55          |
| 10.2 Security assurance requirements rationale.....             | 61          |
| <b>Bibliography</b> .....                                       | <b>63</b>   |

## European foreword

This document (EN 419231:2019) 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 February 2020, and conflicting national standards shall be withdrawn at the latest by February 2020.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

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 organisations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

## Introduction

This document specifies a protection profile for a software component that is part of time stamping system that provides time-stamp tokens to requesters. The TOE operational environment is composed of an operating system, other software applications, drivers and an external UTC time source that is considered to be trusted by the TOE. When a cryptographic module is being used, it is outside of the TOE perimeter.

The TOE is expected to be protected by physical and organisational protection measures implemented by the TOE environment. Those measures are expected to restrict the TOE physical access (e.g. for administration purposes) to authorized persons only and are expected to require dual control. ETSI EN 319 421 specifies additional policy and security requirements relating to the operation and management practices of TSPs issuing time-stamps.

This protection profile is issued by the European Committee for Standardization, Information Society Standardization System (CEN/ISSS).

Correspondence and comments to this document should be referred to:

**Editor: Dr. Jorge López Hernández-Ardieta**

**Email:** [jlhardieta@indra.es](mailto:jlhardieta@indra.es)

**Main contributor: Mr. Julien Gros Lambert**

**Email:** [julien.gros Lambert@mybusinesseducation.fr](mailto:julien.gros Lambert@mybusinesseducation.fr)

After EN approval the contact address will be:

**CEN/ISSS Secretariat**

**Rue de Stassart 36**

**1050 Brussels, Belgium**

**Tel +32 2 550 0813**

**Fax +32 2 550 0966**

**Email:** [iss@cenorm.be](mailto:iss@cenorm.be)

For Revision history, see Annex A.

For document structure, see Annex B.

# 1 Scope

This document specifies a protection profile for trustworthy systems supporting time stamping.

# 2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

CEN/TS 419221-2, *Protection Profiles for TSP cryptographic modules - Part 2: Cryptographic module for CSP signing operations with backup*

CEN/TS 419221-4, *Protection Profiles for TSP cryptographic modules - Part 4: Cryptographic module for CSP signing operations without backup*

EN 419221-5, *Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services*

ISO/IEC 15408 (all parts),<sup>1</sup> *Information technology — Security techniques — Evaluation criteria for IT security*

ISO/IEC 19790, *Information technology — Security techniques — Security requirements for cryptographic modules*

ETSI EN 319 421:2016, *Electronic Signatures and Infrastructures (ESI) - Policy and Security Requirements for Trust Service Providers providing Time-Stamping*

# 3 Terms, definitions and abbreviations

## 3.1 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at <http://www.electropedia.org/>
- ISO Online browsing platform: available at <https://www.iso.org/obp>

### 3.1.1

#### Coordinated Universal Time

#### UTC

time scale based on the second as defined in TF.460-6

Note 1 to entry: For most practical purposes UTC is equivalent to mean solar time at the prime meridian (0°). More specifically, UTC is a compromise between the highly stable atomic time (Temps Atomique International - TAI) and solar time derived from the irregular Earth rotation (related to the Greenwich mean sidereal time (GMST) by a conventional relationship).

<sup>1</sup> The following documents are equivalent to ISO/IEC 15408:

Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; Version 3.1, Revision 4. CCMB-2012-09-002, September 2012.

Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; Version 3.1, Revision 4. CCMB-2012-09-003, September 2012.