This is a free page sample. Access the full version online.

NSAI Standards

Irish Standard
I.S. EN 419231:2019

Protection profile for trustworthy systems supporting time stamping

© CEN 2019 No copying without NSAI permission except as permitted by copyright law.

This is a free page sample. Access the full version online.

I.S. EN 419231:2019

Incorporating amendments/corrigenda/National Annexes issued since publication:

The National Standards Authority of Ireland (NSAI) produces the following categories of formal documents:

I.S. xxx: Irish Standard — national specification based on the consensus of an expert panel and subject to public consultation.

S.R. xxx: Standard Recommendation — recommendation based on the consensus of an expert panel and subject to public consultation.

SWiFT xxx: A rapidly developed recommendatory document based on the consensus of the participants of an NSAI workshop.

This document replaces/revises/consolidates the NSAI adoption of the document(s) indicated on the CEN/CENELEC cover/Foreword and the following National document(s):

NOTE: The date of any NSAI previous adoption may not match the date of its original CEN/CENELEC document.

This document is based on:	*Published:*
EN 419231:2019	2019-08-29

This document was published under the authority of the NSAI and comes into effect on:	ICS number:
2019-09-15	35.030 35.040.01
	NOTE: If blank see CEN/CENELEC cover page

NSAI	T +353 1 807 3800	Sales:
1 Swift Square,	F +353 1 807 3838	T +353 1 857 6730
Northwood, Santry	E standards@nsai.ie	F +353 1 857 6729
Dublin 9	W NSAI.ie	W standards.ie

Údarás um Chaighdeáin Náisiúnta na hÉireann

This is a free page sample. Access the full version online.

National Foreword

I.S. EN 419231:2019 is the adopted Irish version of the European Document EN 419231:2019, Protection profile for trustworthy systems supporting time stamping

This document does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

For relationships with other publications refer to the NSAI web store.

Compliance with this document does not of itself confer immunity from legal obligations.

In line with international standards practice the decimal point is shown as a comma (,) throughout this document.

This is a free page sample. Access the full version online.

This page is intentionally left blank

This is a free page sample. Access the full version online.

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 419231

August 2019

ICS 35.030; 35.040.01

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

© 2019 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

Ref. No. EN 419231:2019 E

This is a free page sample. Access the full version online.

Contents

Page

European foreword ... 3

Introduction ... 4

1 Scope ... 5

2 Normative references ... 5

3 Terms, definitions and abbreviations ... 5
3.1 Terms and definitions ... 5
3.2 Abbreviations ... 11

4 Introduction ... 12
4.1 PP reference ... 12
4.2 TOE overview ... 12

5 Conformance claims ... 18
5.1 CC conformance claim ... 18
5.2 PP claim ... 18
5.3 Conformance rationale ... 18
5.4 Conformance statement ... 18

6 Security problem definition ... 19
6.1 TOE assets ... 19
6.2 Threats ... 21
6.3 Organizational security policies ... 24
6.4 Assumptions ... 25

7 Security objectives ... 27
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

8 Security functional requirements ... 37
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

9 Security assurance requirements ... 54

10 Security requirements rationale ... 55
10.1 Security functional requirements rationale ... 55
10.2 Security assurance requirements rationale ... 61

Bibliography ... 63

This is a free page sample. Access the full version online.

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.

This is a free page sample. Access the full version online.

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

Main contributor: Mr. Julien Groslambert

Email: julien.groslambert@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: isss@cenorm.be

For Revision history, see Annex A.

For document structure, see Annex B.

This is a free page sample. Access the full version online.

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),[1] *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).

[1] 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.

SAI GLOBAL

This is a free preview. Purchase the entire publication at the link below:

Product Page

Looking for additional Standards? Visit Intertek Inform Infostore

Learn about LexConnect, All Jurisdictions, Standards referenced in Australian legislation