SLOVENSKI STANDARD
SIST EN 419231:2019

01-november-2019

Profil zaščite zaupanja vrednih sistemov, ki podpirajo časovne žige

Protection profile for trustworthy systems supporting time stamping

Schutzprofil für vertrauenswürdige Systeme, die Zeitstempel unterstützen

Profil de protection pour systèmes fiables d'horodatage

Ta slovenski standard je istoveten z: **EN 419231:2019**

ICS:

35.030	Informacijska varnost	IT Security
35.040.01	Kodiranje informacij na splošno	Information coding in general

SIST EN 419231:2019 **en,fr,de**

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

Ref. No. EN 419231:2019 E

Contents

Page

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

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.

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.

3.1.2
requester
legal or natural person to whom a time-stamp token is issued and who is bound to any requester obligations

3.1.3
time-stamping policy
named set of rules that indicates the applicability of a time-stamp token to a particular community and/or class of application with common security requirements

3.1.4
time-stamp token
data object that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed before that time

3.1.5
time-stamping authority
TSA
authority which issues time-stamp tokens using one or more time stamping units (TSUs)

3.1.6
time-stamping unit
TSU
set of hardware and software which is managed as a unit and has a single time-stamp token signing key active at a time

3.1.7
TSA system
composition of IT products and components organized to support the provision of time-stamping services

3.1.8
time-stamping service
service that generates and provides time-stamp tokens

3.1.9
electronic signature
data in electronic form which is attached to or logically associated with other electronic data in electronic form and which is used by the signatory to sign

[SOURCE: Reg. eIDAS]

3.1.10
advanced electronic signature
electronic signature which meets the following requirements:

a) it is uniquely linked to the signatory;

b) it is capable of identifying the signatory;

c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and

d) it is linked to the data signed therewith in such a way that any subsequent change in the data are detectable

[SOURCE: Reg. eIDAS modified]

3.1.11
qualified electronic signature
advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures

[SOURCE: Reg. eIDAS]

3.1.12
signatory
natural person who creates an electronic signature

[SOURCE: Reg. eIDAS]

3.1.13
electronic signature-creation data
unique data which is used by the signatory to create an electronic signature

[SOURCE: Reg. eIDAS]

3.1.14
electronic signature-creation device
configured software or hardware used to create an electronic signature

[SOURCE: Reg. eIDAS]

3.1.15
qualified electronic- signature-creation device
electronic signature creation device that meets the requirements in Annex II of eIDAS Regulation

[SOURCE: Reg. eIDAS modifed]

3.1.16
signature-verification-data or validation data
data that is used to validate an electronic signature or an electronic seal

[SOURCE: Reg. eIDAS]

3.1.17
certificate for electronic signature
electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person

[SOURCE: Reg. eIDAS]

3.1.18
qualified certificate for electronic signature
certificate for electronic signatures that is issued by a qualified trust service provider and meets the requirements laid down in Annex I of eIDAS Regulation

[SOURCE: Reg. eIDAS modified]

3.1.19
certification-service-provider
electronic service normally provided for remuneration which consists of issuance of certificates related to the services of creation, verification, and validation of electronic signatures and electronic seals

[SOURCE: Reg. eIDAS modified]

3.1.20
trustworthy system
information system or product implemented as either hardware and/or software that produces reliable and authentic records which are protected against modification and additionally ensures the technical and cryptographic security of the processes supported by it

3.1.21
self-signed certificate
certificate for one CA signed by that CA

[SOURCE: RFC 5280]

3.1.22
certificate policy
named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements

[SOURCE: ISO/IEC 9594-8; ITU-T X.509]

3.1.23
certification authority (CA)
authority trusted by one or more users to create and assign certificates. Optionally the certification authority may create the users' keys

[SOURCE: ISO/IEC 9594-8; ITU-T X.509]

3.1.24
end entity
certificate subject which uses its private key for purposes other than signing certificates

[SOURCE: ISO/IEC 9594-8; ITU-T X.509]

3.1.25
relying party
user or agent that relies on the data in a certificate in making decisions

[SOURCE: RFC 5280]

3.1.26
security policy
set of rules laid down by the security authority governing the use and provision of security services and facilities

[SOURCE: ISO/IEC 9594-8; ITU-T X.509]

3.1.27
activation data
data values, other than keys, that are required to operate cryptographic devices and that need to be protected (e. g., a PIN, a passphrase, or a manually-held key share)

[SOURCE: RFC 3647]

3.1.28
public key
that key of an entity's asymmetric key pair which can be made public

[SOURCE: ISO/IEC 9798-1]

3.1.29
private key
that key of an entity's asymmetric key pair which should only be used by that entity

[SOURCE: ISO/IEC 9798-1]

3.1.30
hash function
function which maps string of bits to fixed-length strings of bits, satisfying the following two properties:

a) it is computationally infeasible to find for a given output an input which maps to this output;

b) it is computationally infeasible to find for a given input a second input which maps to the same output

[SOURCE: ISO/IEC 10118-1]

3.1.31
digital signature
data appended to, or a cryptographic transformation (see cryptography) of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient

[SOURCE: ISO 7498-2:1989]

3.1.32
authentication data
data used to verify the claimed identity of a user requesting services from TWS

3.1.33
subject
entity identified in a certificate as the holder of the private key associated with the public key given in the certificate

3.1.34
registration service
service that verifies the identity and, if applicable, any specific attributes of a subject

Note 1 to entry: The results of this service are passed to the Certificate Generation Service

3.1.35
certificate generation service
service that creates and sign certificates based on the identity and other attributes verified by the registration service

3.1.36
dissemination service
service that disseminates certificates to subjects, and if the subject consents, to relying parties as well as the CA's policy & practice information to subjects and relying parties

3.1.37
revocation management service
service that processes requests and reports relating to revocation to determine the necessary action to be taken

Note 1 to entry: The results of this service are distributed through the Revocation Status Service

3.1.38
revocation status service
service that provides certificate revocation status information to relying parties; this service may be a real-time service or may be based on revocation status information which is updated at regular intervals

3.1.39
cryptographic device
hardware-based cryptographic device that generates stores and protects cryptographic keys and provides a secure environment in which to perform cryptographic functions

3.1.40
subject device provision service
service that prepares and provides a signature creation device to subjects

3.2 Abbreviations

For the purposes of this document, the following abbreviations apply.

ARL	Authority Revocation List
CA	Certification Authority
CEN	Comité Européen de Normalisation (European Committee for Standardization)
CEN/ISSS	CEN Information Society Standardization System
CP	Certificate Policy
CRL	Certificate Revocation List
CSP	Certification Service Provider
EC	European Commission
EESSI	European Electronic Signature Standardization Initiative
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
ISSS	Information Society Standardization System
NQC	Non-Qualified Certificate
OCSP	Online Certificate Status Protocol
OS	Operating System
OSP	Organisational Security Policy
PKI	Public Key Infrastructure
PP	Protection Profile
QC	Qualified Certificate
SCDev	Signature-Creation Device
SSCD	Secure-Signature-Creation Device
ST	Security Target
TSA	Time-Stamping Authority
TSP	Trust Service Provider
TSS	Time-Stamping Service
TST	Time-Stamp Token
TWS	Trustworthy System
WORM	Write Once Read Many
WS/E-SIGN	CEN/ISSS Electronic Signatures workshop

4 Introduction

4.1 PP reference

Title:	Protection profile for trustworthy systems supporting time stamping
Authors:	Jorge López Hernández-Ardieta, Julien Groslambert
Version:	0,17
Publication date:	24th September 2018

4.2 TOE overview

4.2.1 TOE type

The TOE corresponds to a software component running on an operating system and that provides time-stamps generation services to its requesters. Hardware and other software components (e.g. operating system, drivers, and other software applications) that might be needed by the TOE to provide its services are considered part of the TOE operational environment. The TOE shall use a hardware secure module (HSM) for the implementation of the cryptographic operations.

4.2.2 TOE usage and major security features

The TOE is a software component that provides services for the generation of time-stamps in a manner that:

— It is able to receive and process time-stamping requests from external users (requesters), protecting the integrity of the requests when managed by the TOE.

— The integrity of the time-stamps produced by the TOE is protected when created and managed by the TOE and during transfer from the TOE to an external entity.

— Any external entity can verify the authentication of the time-stamps produced by the TOE.

— The TOE services (user identity and role management, TSU initialisation, start of TSU operation, stop of TSU operation, finalisation of TSU operation, generation of key pair, public key export for certificate request, certificate import, timestamp token generation and internal audit) are only used in an authorized way.

— The time included in the time-stamps is synchronised with a trusted UTC time source.

The TOE shall provide the following additional functions to protect the TOE services:

— User authentication and access control, except for requesters (see roles below).

— Auditing of security-relevant events produced within the TOE boundaries.

The TOE shall handle the following user data:

— Time-stamping request: Time-stamping request sent by the requester to the TOE in order to obtain a time-stamp.

— Time-stamp: Time-stamp generated and signed by the TOE based on the time-stamp request information, and using the active private key of the time stamping context of the TSU.

— Time-stamp context: Set of data that comprises all the information needed to operate a TSU.

- Internal clock: Internal time used by the TSU that provides the date and time corresponding to UTC time included in each time-stamp.

- Cryptographic key pair: Public key used by external entities to verify the integrity and origin authentication of the TOE signed time-stamps, and handler to the private key used by the TSU to digitally sign the time-stamps.

- Audit data: Internal audit records produced by the TOE.

The TOE shall, as a minimum, support the following user categories (roles):

- Requester of the TOE services: external entity that sends time-stamping requests to the TOE and expects to receive a time-stamp signed by the TOE.

- Security Officer: Overall responsibility for administering the implementation of the security practices as well as administering the TSU.

- System Administrator: Authorized to install, configure and maintain the TOE and the trustworthy systems of the operational environment for time-stamping management.

- System Operator: Responsible for operating the TOE and the trustworthy systems of the operational environment on a day-to-day basis. Authorized to perform system backup and recovery.

- System Auditor: Authorized to view archives and audit logs of the TOE and the trustworthy systems of the operational environment.

Any user accessing the time-stamp generation service is regarded as a Requester. This service may be not authenticated and there may be no access control mechanism. Notwithstanding, the TOE will not process the authentication data, and thus the requests will be treated as non-authenticated.

The TOE may support other roles or sub-roles in addition to the roles specified above. The roles may also be allowed to perform additional functions provided by the TOE as long as the separation between different roles is given. None of those additional roles shall be able to access the security-related and management services restricted to the Security Officer role.

The interface to the TOE may be either shared between the different user categories, or separated for certain functions. Authentication for all user categories shall be identity-based, except for the Requester, who accesses non-authenticated services.

Figure 1 shows an overview of the TOE and its relations with the operational environment and TOE users.