

DIN EN 419231

ICS 35.030; 35.040.01

Einsprüche bis 2017-05-31

Entwurf**Schutzprofil für vertrauenswürdige Systeme die Zeitstempel unterstützen;
Englische Fassung prEN 419231:2017**

Protection Profile for trustworthy systems supporting time stamping;
English version prEN 419231:2017

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2017-03-31 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), 10772 Berlin, Burggrafenstr. 6, 10787 Berlin.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 72 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Dieses Dokument (prEN 419231:2017) wurde vom Technischen Komitee CEN/TC 224 „Persönliche Identifikation, elektronische Signatur, maschinenlesbare Karten sowie zugehörige Geräteschnittstellen und Verfahren“ erarbeitet, dessen Sekretariat von AFNOR (Frankreich) gehalten wird.

Das zuständige deutsche Normungsgremium ist der Unterausschuss NA 043-01-17-04 UA „Austauschprotokolle bei Chipkarten“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

Dieses Dokument wurde unter einem Mandat erarbeitet, das die Europäische Kommission und die Europäische Freihandelszone dem CEN erteilt haben.

Diese Europäische Norm definiert ein Schutzprofil für eine Softwarekomponente, die zu einem Zeitstempelsystem gehört, welches Zeitstempel-Token für Antragsteller zur Verfügung stellt. Die Einsatzumgebung des Evaluierungsgegenstandes (EVG, en: Target of Evaluation, TOE) besteht aus einem Betriebssystem, anderen Softwareanwendungen, Treibern und einer externen UTC Zeitquelle, die vom EVG als vertrauenswürdig angesehen wird. Ein verwendetes kryptographisches Modul ist außerhalb der EVG-Umgebung.

Der EVG wird durch physische und organisatorische Maßnahmen, die von der EVG Umgebung implementiert werden, geschützt. Diese Maßnahmen sollen den physischen Zugang zum EVG (z. B. zu Verwaltungszwecken) auf autorisierte Personen beschränken und benötigen eine Vier-Augen Kontrolle. ETSI EN 319421 definiert zusätzliche Richtlinien- und Sicherheitsanforderungen im Bezug auf die Betriebs- und Verwaltungsmethoden von Zeitstempel ausgebenden Vertrauensdiensteanbietern.

Das Präsidium des DIN hat mit seinem Beschluss 1/2004 festgelegt, dass von dem in den Regeln der europäischen Normungsarbeit von CEN/CENELEC verankerten Grundsatz, wonach Europäische Normen in den drei offiziellen Sprachen Deutsch, Englisch, Französisch veröffentlicht werden, in begründeten Ausnahmefällen abgewichen und auf die deutsche Sprachfassung verzichtet werden kann. Daher wurden von dieser Norm nur die Begriffe übersetzt (siehe Nationaler Anhang NA).

Nationaler Anhang NA (informativ)

Begriffe und Abkürzungen

NA.1 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

3.1.1

Koordinierte Weltzeit (UTC)

Zeitskala auf Basis von Sekunden, wie in TF.460.6 definiert

Anmerkung 1 zum Begriff: Aus praktischen Gründen entspricht UTC der mittleren Sonnenzeit am Nullmeridian (0°). Genauer gesagt ist UTC ein Kompromiss zwischen der hochstabilen Atomzeit (fr: Temps Atomique International – TAI) und der Sonnenzeit abgeleitet von der unregelmäßigen Erdrotation (bezogen auf die mittlere Greenwich Sternzeit (GMST, en: Greenwich mean sidereal time) durch eine konventionelle Beziehung)

3.1.2

Antragsteller

juristische oder natürliche Person, der ein Zeitstempel-Token ausgestellt wird und die an jegliche Antragstellerverpflichtungen gebunden ist

3.1.3

Zeitstempelrichtlinie

definierter Regelsatz, der die Anwendbarkeit eines Zeitstempel-Token für eine bestimmte Gemeinschaft und/oder eine Anwendungsklasse mit allgemeinen Sicherheitsanforderungen angibt

3.1.4

Zeitstempel-Token

Datenobjekt, welches ein Datum mit einer bestimmten Zeit verknüpft und dadurch den Nachweis erbringt, dass das Datum vor diesem Zeitpunkt vorhanden war

3.1.5

Zeitstempelstelle

TSA

Autorität, die Zeitstempel-Token unter Verwendung einer oder mehrerer Zeitstempелеinheiten (TSUs) ausgibt

3.1.6

Zeitstempелеinheit

TSU

Reihe von Hardware und Software, die als eine Einheit verwaltet wird und die zu einem Zeitpunkt nur einen aktiven Zeitstempel-Token Signierschlüssel hat

3.1.7

TSA System

Zusammensetzung von IT- Produkten und Komponenten, die zur Unterstützung der Bereitstellung von Zeitstempeldiensten organisiert werden

3.1.8

Zeitstempeldienst

Dienst, der Zeitstempel-Token erzeugt und bereitstellt

3.1.9

elektronische Signatur

Daten in elektronischer Form, die anderen elektronischen Daten beigelegt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dieser Daten dienen

[QUELLE: Dir.1999/93/EU]

3.1.10

fortgeschrittene elektronische Signatur

elektronische Signatur, die

- a) ausschließlich dem Unterzeichner zugeordnet ist;
- b) die Identifizierung des Unterzeichners ermöglicht;
- c) mit Mitteln erstellt wird, die der Unterzeichner unter seiner alleinigen Kontrolle halten kann;
- d) so mit den Daten, auf die sie sich bezieht, verknüpft ist, dass eine nachträgliche Veränderung der Daten erkannt werden kann

[QUELLE: Dir.1999/93/EU]

3.1.11

qualifizierte elektronische Signatur

fortgeschrittene elektronische Signatur, die auf einem qualifizierten Zertifikat beruht und von einer sicheren Signaturerstellungseinheit erstellt wird

3.1.12

Unterzeichner

Person, die Signaturstellungsdaten besitzt und die entweder im eigenen Namen oder im Namen der natürlichen oder juristischen Person oder der von ihr vertretenen Stelle handelt

[QUELLE: Dir.1999/93/EU]

3.1.13

Signaturstellungsdaten

einmalige Daten wie Codes oder private kryptographische Schlüssel, die vom Unterzeichner zur Erstellung einer elektronischen Signatur verwendet werden

[QUELLE: Dir.1999/93/EU]

3.1.14

Signaturerstellungseinheit

konfigurierte Software oder Hardware, die zur Implementierung der Signaturstellungsdaten verwendet wird

[QUELLE: Dir.1999/93/EU]

3.1.15

Sichere Signaturerstellungseinheit

Signaturerstellungseinheit, die die Anforderungen des Anhangs III erfüllt

[QUELLE: Dir.1999/93/EU]

3.1.16

Signaturprüfdaten

Daten wie Codes oder öffentliche kryptographische Schlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden

[QUELLE: Dir.1999/93/EU]

3.1.17

Zertifikat

elektronische Bescheinigung, mit der Signaturprüfdaten einer Person zugeordnet werden und die Identität dieser Person bestätigt wird

[QUELLE: Dir.1999/93/EU]

3.1.18

qualifiziertes Zertifikat

Zertifikat, das die Anforderungen des Anhangs I der Richtlinie erfüllt und von einem Zertifizierungsdiensteanbieter bereitgestellt wird, der die Anforderungen des Anhangs II der Richtlinie erfüllt

[QUELLE: Dir.1999/93/EU]

3.1.19

Zertifizierungsdiensteanbieter

Stelle oder eine juristische oder natürliche Person, die Zertifikate ausstellt oder anderweitige Dienste im Zusammenhang mit elektronischen Signaturen bereitstellt

[QUELLE: Dir.1999/93/EU]

3.1.20

vertrauenswürdiges System

als Hardware und/oder Software implementiertes Informationssystem oder -produkt, das zuverlässige und authentische Aufzeichnungen erzeugt, die gegen Veränderungen geschützt sind, und zusätzlich die technische und kryptographische Sicherheit der von ihm unterstützten Prozesse sicherstellt

3.1.21

selbst-signiertes Zertifikat

Zertifikat für eine CA, die durch diese CA signiert wurde

[QUELLE: RFC 5280]

3.1.22

Zertifikatrichtlinie

benannter Satz von Regeln, der die Anwendbarkeit eines Zertifikats auf eine bestimmte Gemeinschaft und/oder Anwendungsklasse mit gemeinsamen Sicherheitsanforderungen angibt

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

3.1.23

Zertifizierungsstelle

CA

Stelle, die durch einen oder mehrere Benutzer damit betraut wird, Zertifikate zu erstellen und zuzuordnen und die wahlweise Schlüssel für die Benutzer erstellen darf

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

3.1.24

End-Entität

Zertifikatinhaber, der seinen privaten Schlüssel für andere Zwecke als das Signieren von Zertifikaten nutzt

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

3.1.25

vertrauende Partei

Benutzer oder dessen Vertreter, der sich bei der Entscheidungsfindung auf die Daten in einem Zertifikat verlässt

[QUELLE: RFC 5280]

3.1.26

Sicherheitsrichtlinie

Satz von Regeln, der durch die Sicherheitsbehörde festgelegt wurde und die Nutzung und Bereitstellung von Sicherheitsdiensten und -einrichtungen regelt

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

3.1.27

Aktivierungsdaten

Datenwerte, bei denen es sich nicht um Schlüssel handelt und die für den Betrieb kryptographischer Einheiten erforderlich sind und geschützt werden müssen (z. B. eine PIN, eine Passphrase oder ein manuell gehandhabter Schlüsselanteil)

[QUELLE: RFC 3647]

3.1.28

öffentlicher Schlüssel

Schlüssel eines asymmetrischen Schlüsselpaares einer Entität, der öffentlich gemacht werden kann

[QUELLE: ISO/IEC 9798-1]

3.1.29

privater Schlüssel

Schlüssel eines asymmetrischen Schlüsselpaares einer Entität, der nur durch diese Entität genutzt werden sollte

[QUELLE: ISO/IEC 9798-1]

3.1.30

Hash-Funktion

Funktion, die Bitfolgen auf Bitfolgen fester Länge abbildet und für die es:

- a) rechnerisch unmöglich ist, für eine gegebene Ausgabe eine Eingabe zu finden, die auf diese Ausgabe abbildbar ist;
- b) rechnerisch unmöglich ist, für eine gegebene Eingabe eine zweite Eingabe zu finden, die auf dieselbe Ausgabe abbildbar ist.

[QUELLE: ISO/IEC 10118-1]

3.1.31

digitale Signatur

an eine Dateneinheit angehängte Daten oder eine kryptographische Umwandlung (siehe Kryptographie) dieser Dateneinheit, die es einem Empfänger der Dateneinheit erlauben/erlaubt, die Quelle und Integrität der Dateneinheit nachzuweisen, und die einen Schutz gegen Fälschung, zum Beispiel durch den Empfänger, bieten/bietet

[QUELLE: ISO 7498-2:1989]

3.1.32

Authentisierungsdaten

Daten, die zur Überprüfung der behaupteten Identität eines Benutzers, der Dienste vom vertrauenswürdigen System anfordert, verwendet werden

3.1.33

Zertifikatinhaber

in einem Zertifikat als der Inhaber des privaten Schlüssels identifizierte Entität, der mit dem öffentlichen Schlüssel im Zertifikat assoziiert wird

3.1.34

Registrierungsdienst

Dienst, der die Identität und gegebenenfalls jegliche spezifischen Attribute eines Zertifikatinhabers überprüft

3.1.35

Zertifikatausstellungsdienst

Dienst, der auf der Grundlage der Identität und weiterer, durch den Registrierungsdienst überprüfter Attribute Zertifikate erstellt und signiert

3.1.36

Ausgabedienst

Dienst, der Zertifikate an Zertifikatinhaber sowie, bei Einverständnis der Zertifikatinhaber, an vertrauende Parteien übermittelt

Anmerkung 1 zum Begriff: Der Dienst übermittelt auch die Informationen zu den Grundsätzen und Betriebspraktiken der CA an die Zertifikatinhaber und vertrauenden Parteien.

3.1.37

Sperrdienst

Dienst, der Anfragen und Berichte im Zusammenhang mit Sperrungen bearbeitet, um die erforderlichen Maßnahmen zu bestimmen

Anmerkung 1 zum Begriff: Die Ergebnisse dieses Dienstes werden an den Sperrstatusdienst übermittelt.

3.1.38

Sperrstatusdienst

Dienst, der vertrauenden Parteien Informationen zum Zertifikatsperrstatus bereitstellt und der ein Echtzeitdienst sein oder auf Informationen zum Sperrstatus beruhen darf, die regelmäßig aktualisiert werden

3.1.39

kryptografische Einheit

hardwarebasierte kryptographische Einheit, die kryptographische Schlüssel erzeugt, speichert und schützt sowie eine sichere Umgebung für die Ausführung kryptographischer Funktionen bietet

3.1.40

Bereitstellungsdienst für Signaturerstellungseinheiten für Zertifikatinhaber

Dienst, der Signaturerstellungseinheiten herstellt und sie Zertifikatinhabern bereitstellt

NA.2 Abkürzungen

Für die Anwendung dieses Dokuments gelten die folgenden Abkürzungen.

ARL	Sperrliste mit Zertifikaten der ausgebenden Stelle (en: Authority Revocation List)
CA	Zertifizierungsstelle (en: Certification Authority)
CEN	Europäisches Komitee für Normung (fr: Comité Européen de Normalisation)
CEN/ISSS	Normungssystem für die Informationsgesellschaft im CEN (en: CEN Information Society Standardization System)
CP	Zertifizierungsrichtlinie (en: Certificate Policy)
CRL	Zertifikatssperrliste (en: Certificate Revocation List)
CSP	Zertifizierungsdiensteanbieter (en: Certification Service Provider)
EC	Europäische Kommission (en: European Commission)
EESSI	Europäische Initiative zur Normung elektronischer Signaturen (en: European Electronic Signature Standardization Initiative)
ETSI	Europäisches Institut für Telekommunikationsnormen (en: European Telecommunications Standards Institute)
ISSS	Normungssystem für die Informationsgesellschaft (en: Information Society Standardisation System)
NQC	Nicht qualifiziertes Zertifikat (en: Non-Qualified Certificate)
OCSP	Online-Zertifikatsstatusprotokoll (en: Online Certificate Status Protocol)
OS	Betriebssystem (en: Operating System)
PKI	Public Key Infrastruktur (en: Public Key Infrastructure)
PP	Schutzprofil (en: Protection Profile)
QC	Qualifiziertes Zertifikat (en: Qualified Certificate)
SCDev	Signaturerstellungseinheit (en: Signature-Creation Device)
SSCD	Sichere Signaturerstellungseinheit (en: Secure-Signature-Creation Device)
TSA	Zeitstempelstelle (en: Time-Stamping Authority)
TSP	Vertrauensdiensteanbieter (en: Trust Service Provider)
TSS	Zeitstempeldienst (en: Time-Stamping Service)
TST	Zeitstempel-Token (en: Time-Stamping Token)
TWS	Vertrauenswürdiges System (en: Trustworthy System)
WORM	einmal beschreibbar, mehrfach lesbar (en: Write Once Read Many)
WS/E-SIGN	CEN/ISSS Workshop „Elektronische Signaturen“ (en: CEN/ISSS Electronic Signatures workshop)

English Version

Protection profile for trustworthy systems supporting time stamping

Schutzprofil für vertrauenswürdige Systeme die
Zeitstempel unterstützen

This draft European Standard is submitted to CEN members for enquiry. It has been drawn up by the Technical Committee CEN/TC 224.

If this draft becomes a European Standard, 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.

This draft European Standard was established by CEN 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, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Contents

Page

European foreword.....	4
Introduction	5
1 Scope	6
2 Normative references	6
3 Terms and definitions	6
3.1 Definitions	6
3.2 Abbreviations	11
4 Introduction	12
4.1 PP reference	12
4.2 TOE overview.....	12
4.2.1 TOE type	12
4.2.2 TOE usage and major security features	12
4.2.3 TOE Environment general overview	16
4.2.4 Required non-TOE hardware/software/firmware.....	17
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	18
6.1 TOE assets.....	18
6.2 Threats.....	21
6.2.1 General.....	21
6.2.2 Relation between threats and assets	23
6.3 Organisational security policies	23
6.4 Assumptions.....	24
7 Security objectives.....	26
7.1 General.....	26
7.2 Security objectives for the TOE	26
7.3 Security objectives for the operational environment.....	27
7.4 Security objectives rationale	30
8 Security functional requirements	36
8.1 General.....	36
8.2 Subjects, objects, operations and security attributes	36
8.2.1 Subjects.....	36
8.2.2 Objects.....	37
8.2.3 Operations	37
8.2.4 Security attributes	37
8.3 Security requirements operations.....	39
8.4 User Data Protection (FDP)	39
8.5 Security Management (FMT).....	46
8.6 Protection of the TSF (FPT)	49
8.7 Trusted Path/Channels (FTP).....	49

8.8	Cryptographic Support (FCS).....	50
8.9	Identification and Authentication (FIA)	51
8.10	Security Audit (FAU)	51
9	Security assurance requirements.....	52
10	Security requirements rationale.....	53
10.1	Security functional requirements rationale	53
10.1.1	SFR dependencies rationale	53
10.1.2	SFR vs TOE security objectives rationale	56
10.2	Security assurance requirements rationale	59
10.2.1	General	59
10.2.2	Assurance level table.....	60
10.2.3	EAL rationale	61
	Annex A (informative) Revision History.....	62
	Annex B (informative) Document structure	63
	Bibliography	64

European foreword

This document (prEN 419231:2017) 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 document has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association.

Introduction

This European Standard 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 meant to be protected by physical and organisational protection measures implemented by the TOE environment. Those measures are meant to restrict the TOE physical access (e.g. for administration purposes) to authorized persons only and are meant 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 Gros Lambert

Email: 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: isss@cenorm.be

For Revision history, see Annex A.

For document structure, see Annex B.

1 Scope

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

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.

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*

prEN 419221-5, *Protection profiles for Trust Service Provider Cryptographic modules - Part 5: Cryptographic Module for Trust Services*

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

ISO/IEC 19790:2012, *Information technology – Security techniques – Security requirements for cryptographic modules*

ETSI TS 102 023, *Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authority*

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

3 Terms and definitions

3.1 Definitions

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

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).

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 are attached to or logically associated with other electronic data and which serve as a method of authentication of that data

[SOURCE: Dir.1999/93/EC]

3.1.10

advanced electronic signature

electronic signature which:

- a) is uniquely linked to the signatory;
- b) is capable of identifying the signatory;
- c) is created using means that the signatory can maintain under his sole control; and
- d) is linked to the data to which it relates in such a manner that any subsequent change of the data are detectable

[SOURCE: Dir.1999/93/EC]

3.1.11

qualified electronic signature

advanced electronic signature which is based on a qualified certificate and which is created by a secure-signature-creation device

3.1.12

signatory

person who holds signature-creation data and acts either on his own behalf or on behalf of the natural or legal person or entity he represents

Note 1 to entry: The term signer is sometimes used as a synonym.

[SOURCE: Dir.1999/93/EC]

3.1.13

signature-creation data

unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature

[SOURCE: Dir.1999/93/EC]

3.1.14

signature-creation device

configured software or hardware used to implement the signature-creation data

[SOURCE: Dir.1999/93/EC]

3.1.15

secure-signature-creation device

signature-creation device which meets the requirements laid down in Annex III

[SOURCE: Dir.1999/93/EC]

3.1.16

signature-verification-data

data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature

[SOURCE: Dir.1999/93/EC]

3.1.17

certificate

electronic attestation which links signature-verification-data to a person and confirms the identity of that person

[SOURCE: Dir.1999/93/EC]

3.1.18

qualified certificate

certificate which meets the requirements laid down in Annex I of the Directive and is provided by a certification-service-provider who fulfils the requirements laid down in Annex II of the Directive

[SOURCE: Dir.1999/93/EC]

3.1.19

certification-service-provider

entity or legal or natural person who issues certificates or provides other services related to electronic signatures

[SOURCE: Dir.1999/93/EC]

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

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

[SOURCE: ISO/IEC 9798-1]

3.1.29

private key

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, that is:

- a) computationally infeasible to find for a given output an input which maps to this output;
- b) 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

Note 1 to entry: This service also disseminates 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 Normalization (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
ISSS	Information Society Standardization System

NQC	Non-Qualified Certificate
OCSP	Online Certificate Status Protocol
OS	Operating System
PKI	Public Key Infrastructure
PP	Protection Profile
QC	Qualified Certificate
SCDev	Signature-Creation Device
SSCD	Secure-Signature-Creation Device
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 Gros Lambert
Version:	0.11
Publication date:	19th August 2016

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 should 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.

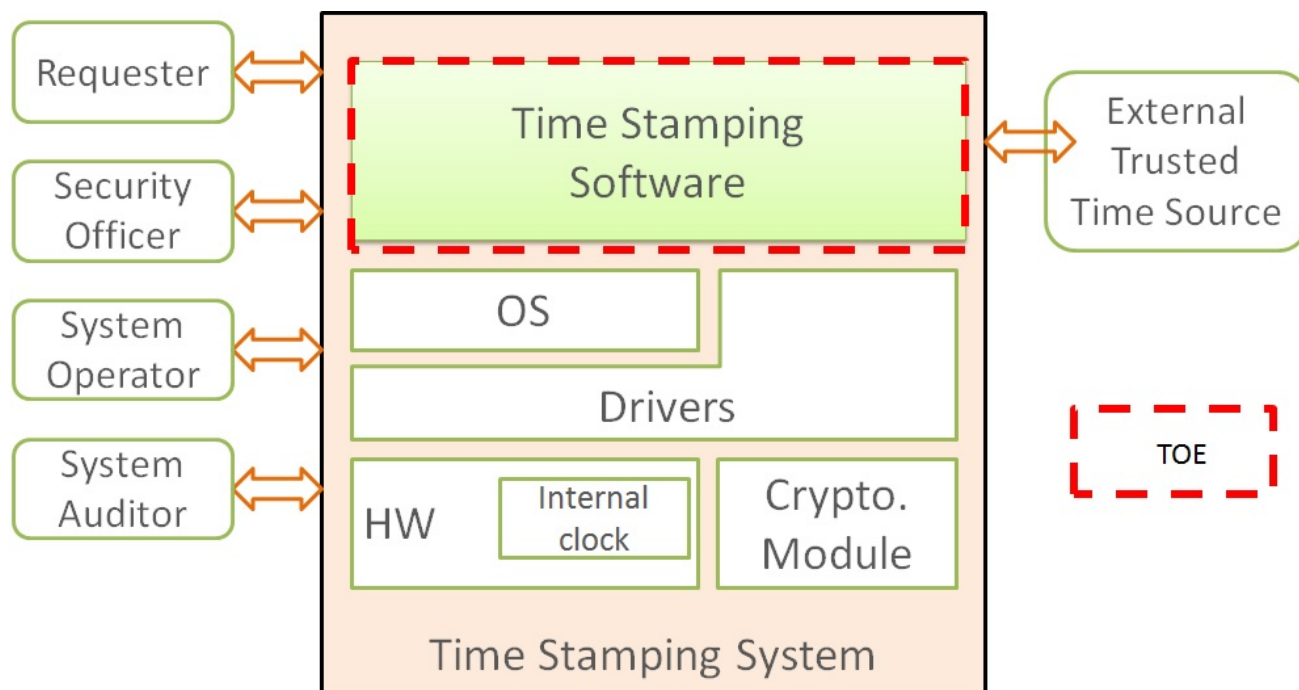


Figure 1 — overview of the TOE and its relations with the operational environment and TOE users

The Time Stamping System is part of the operational environment where the TOE resides. It contains non-TOE elements such as the Operating System or the Cryptographic Module. Figure 2 shows the details of the TOE in terms of functional components that are part of it, as well as the messages/operations exchanged with entities that belong to the operational environment, and others that do not (i.e. the CA, the external trusted time source).