CEN/TC 224

Date: 2013-12

prEN 419231:2013

CEN/TC 224

Secretariat: AFNOR

Protection profile for trustworthy systems supporting time stamping — —

Einführendes Element — —

Élément introductif — —

ICS:

Descriptors:

Document type: European Standard
Document subtype:
Document stage: Working Document
Document language: E

C:\Users\csutter\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\JDELXYNT\EN_419231_(E)_DRAFT_V0.17_ANSSI_comments_CS (004).docx STD Version 2.4a

Contents

Page

Foreword

This document (prEN 419231:2013) 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.

Revision History

PRE-RELEASE HISTORY FOR EDITORIAL TRACKING ONLY, REPLACE FOR FINAL PP

v0.00 07.01.14 initial draft with Introduction and Security Problem Definition sections
v0.01 18.03.14 Terms and definitions, Introduction and Security Problem Definition sections updated. Security Objectives section added.
v0.02 20.05.14 Minor corrections. Rationale for traceability matrix between security objectives and security problem definition added.
v0.03 28.08.14 Added security functional requirements section and corresponding rationale. Applied minor corrections to the security problem definition and security objectives sections.
v0.04 14.11.14 Updated to accommodate changes as agreed during Madrid meeting, 22-23 September 2014.
v0.05 06.01.15 Updated to accommodate changes as agreed during Essen meeting, 2-3 December 2014.
v0.06 20.04.15 Updated to accommodate changes as agreed during London meeting, 4-5 March 2015.
v0.07 20.04.15 Updated to accommodate changes proposed by WG17.
v0.08 11.03.16 Updated to meet issues raised by the evaluation laboratory.
v0.09 17.03.16 Added dual control in access control assumption and OE.
v0.10 14.06.16 Minor changes. Removed FAU_ARP.1 and FAU_SAA.1.
v0.11 19.08.16 Introduction is modified. Security objectives rationale updated. Minor corrections.
v0.12 10.02.17 Minor corrections applied in order to meet comments raised by the Certification Body.
V0.13 27.06.17 Minor modification applied in order to meet comments raised by AFNOR and PKN
v0.14 23.08.18 Editorial corrections following Italian comments
v0.15 23.08.18 Change in A.REF_TIME and elements related to R.KEY_PAIR_PRIV w.r.t. E.T.R
v0.16 14.09.18 Minor editorial change and references to ETSI102023 removed.
v0.17 24.09.18 Further minor editorial changes.

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 shall be protected by physical and organisational protection measures implemented by the TOE environment. Those measures shall restrict the TOE physical access (e.g. for administration purposes) to authorised persons only and shall require dual control. 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).

Document structure

Section 1 provides the scope of the Protection Profile.

Section 2 provides normative references of applicability to this Protection Profile.

Section 3 provides the terms, definitions and abbreviations used along the document.

Section 4 contains the Introduction of the Protection Profile, including the PP reference and the TOE overview.

Section 5 includes the conformance claims for this Protection Profile.

Section 6 contains the security problem definition, including the set of TOE assets to protect, the expected threats to those assets, the organisational security policies in place and the assumptions made on the TOE.

Section 7 contains the security objectives for the TOE and the TOE operational environment, and addresses the threats, organisational security policies and assumptions considered. This section also includes a rational of correspondence between the security objectives and the threats, organisational security policies and assumptions.

Section 8 contains the security functional requirements (SFR) derived from the Common Criteria (CC) Part 2 [ISO/IEC 15408-2], and that shall be satisfied by the TOE. This section introduces first the formalism used to describe the operations (refinement, selection, assignment and iteration) applied, whereas in subsequent subsections the SFR are detailed.

Section 9 describes the security assurance requirements (SAR) according to CC Part 3, and that shall be satisfied by the TOE and the developer.

Section 10 provides the rationale to explicitly demonstrate that the set of SFR are complete with respect to the objectives, and that each security objective is addressed by one or more SFR. Arguments are provided for the coverage of each objective. The rational part also provides a justification for the selection of EAL4+ ALC_FLR.3 as the assurance level.

1 Scope

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

2 References

2.1 Normative references

The following referenced documents are indispensable for the application of this document.

[ITU-460]	ITU-R Recommendation TF.460-6: 2002. Standard-frequency and time-signal emissions.
[ISO/IEC 15408-2]	ISO/IEC 15408-2:2008 Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components.
[ISO/IEC 15408-3]	ISO/IEC 15408-3:2008 Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components.
[EN319421]	EN 319 421 Electronic Signatures and Infrastructures (ESI) - Policy and Security Requirements for Trust Service Providers providing Time-Stamping Services
[ISO/IEC 15408]	ISO/IEC 15408, Information technology - Security techniques - Evaluation criteria for IT security
[FIPS PUB 140-2]	FIPS PUB 140-2, Security requirements for cryptographic modules
[ISO/IEC 19790]	ISO/IEC 19790:2006, Information technology – Security techniques – Security requirements for cryptographic modules.
[CEN TS 419 221-2]	CEN EN 419 221-2. Protection profiles for TSP Cryptographic modules - Part 2: Cryptographic module for CSP signing operations with backup.
[CEN TS 419 221-4]	CEN EN 419 221-4. Protection profiles for TSP Cryptographic modules - Part 4: Cryptographic module for CSP signing operations without backup.
[CEN TS 419 221-5]	CEN EN 419 221-5. Protection profiles for TSP Cryptographic modules - Part 5: Cryptographic module for trust services.

Note: Next documents are equivalent to the aforementioned ISO/IEC 15408 standards:

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.

2.2 Informative references

[ETSI 119 312]	ETSI TS 119 312. Electronic Signatures and Infrastructures (ESI); Cryptographic Suites for Secure Electronic Signatures.
[ETSI 319 411-2]	ETSI EN 319 411-2. Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.
[SOG-IS-Crypto]	SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms. SOG-IS Crypto Working Group. Version 1.0. May 2016.

2.3 Legal references

[Reg. eIDAS]	REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

3 Terms, definitions and abbreviations

3.1 Terms and Definitions

For the purpose of this document, the following terms and definitions apply. Where a definition is copied from a referenced document this is indicated by inclusion of the reference identifier at the end of the definition.

3.1.1
Coordinated Universal Time (UTC)
time scale based on the second as defined in ITU-R Recommendation TF.460-6 [ITU-460].

NOTE: 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 is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;

[SOURCE: Reg. eIDAS]

3.1.10
advanced electronic signature
an 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 is detectable.

[SOURCE: Reg. eIDAS modified]

3.1.11
qualified electronic signature
an 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
a 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
an 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
An 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
an 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. 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. 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. 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

CA	Certification Authority
CEN	Comité Européen de Normalisation (European Committee for Standardization)
CP	Certificate Policy
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
OSP	Organisational Security Policy
ST	Security Target
TOE	Target of Evaluation
TSA	Time-Stamping Authority
TSP	Trust Service Provider
TSS	Time-Stamping Service
TWS	Trustworthy System

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 authorised 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: Authorised 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. Authorised to perform system backup and recovery.

- System Auditor: Authorised 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.

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

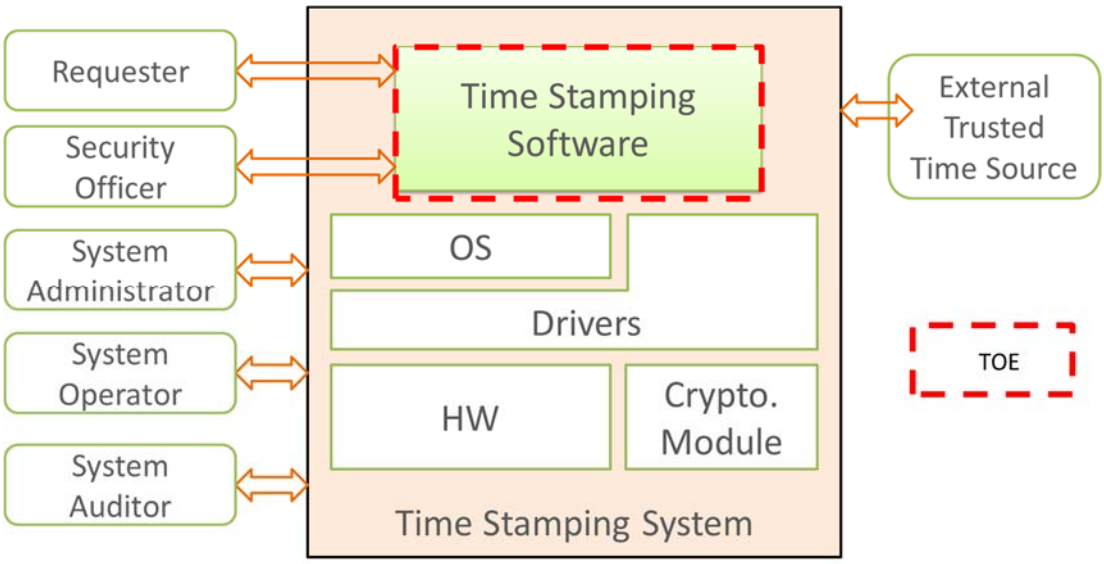

Figure 1. The TOE in its environment

The TOE is a piece of software that is part of a time-stamping system. The time-stamping system is also composed of a computer (typically a server containing hardware, an operating system (OS) and some drivers) running the TOE and a cryptographic module. The TOE is directly interacting with the requester, that exchange with the TOE to obtain timestamps and a Security Officer that is in charge of the configuration of the TOE. The Time Stamping System in general is in interaction with the System Administrator, System Operator and System Auditor on one hand, and an external trusted time source on the other hand.

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. The next Figure 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).

The TOE is composed of three modules (see figure 2):

- A time stamp request manager that handles the exchanges with the requesters (handling Time stamp request and providing corresponding time-stamps.
- A clock manager, in charge of the accurate synchronization with the external Trusted Time Source and the detections of incidents related to the time synchronization.
- A context manager, interacting with the crypto-module and the CA, in charge of the life-cycle of the key pair management. In particular:
    - Requesting the key pair generation within the crypto module;
    - Exporting the public key for the certificate request to the CA;
    - Importing the certificate generated by the CA;
    - Requesting the Crypto module signature of the generated Time-stamps.

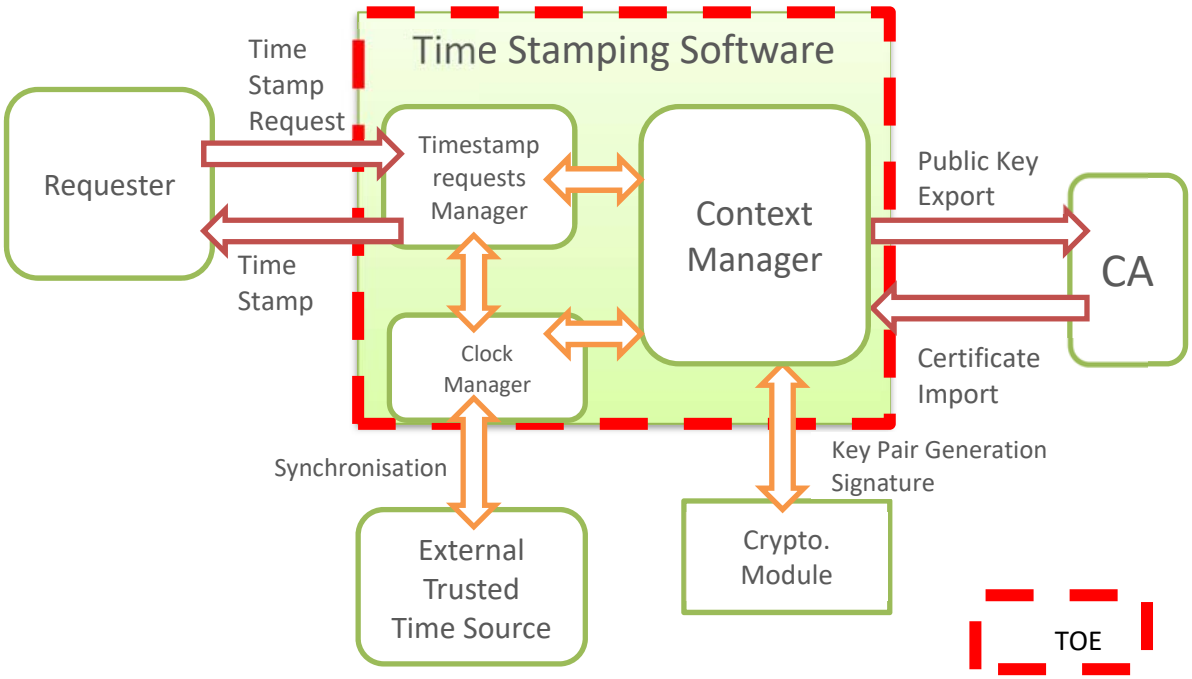

Figure 3 Overview of the TOE functional perimeter.

As can be seen, other entities might be related to the TOE, thought not directly connected through logical interfaces, such as a Certification Authority (CA).

As depicted in the next Figure, the time-stamping software (*i.e.* the TOE) may operate several Time-stamping Units (TSU).

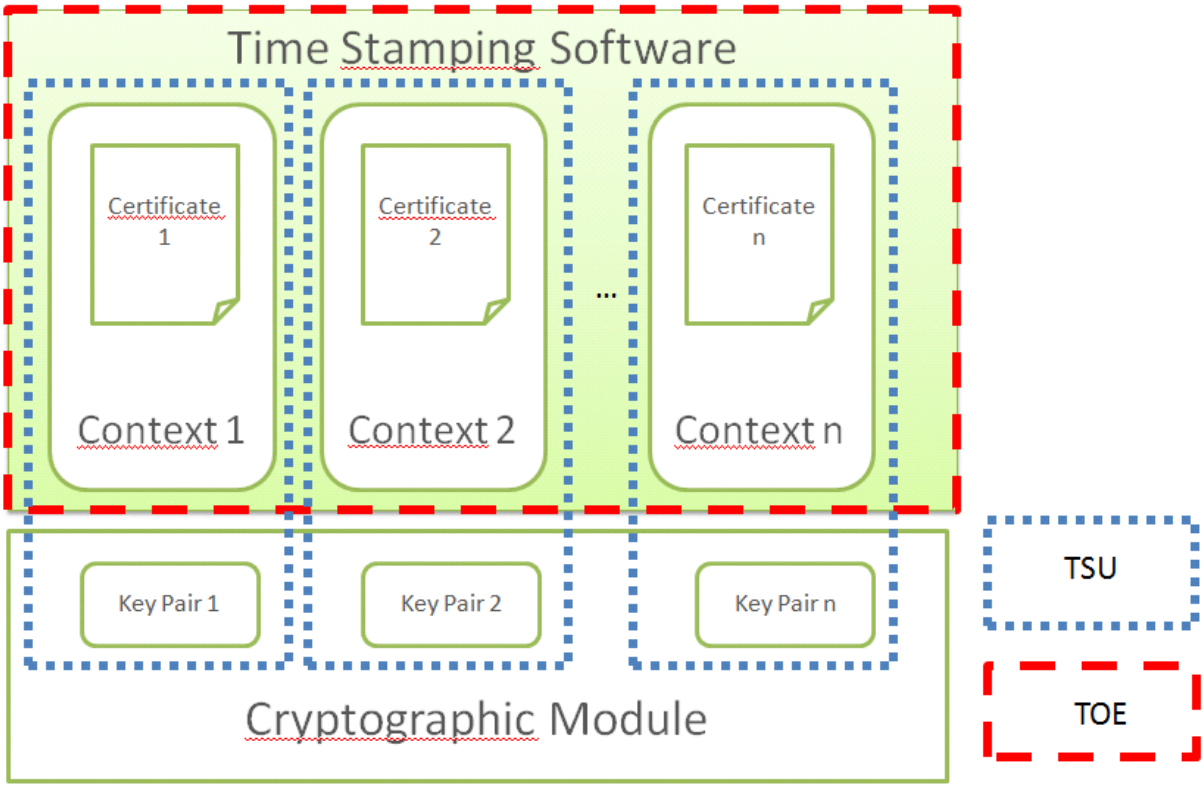

Figure 4. Time-stamping Unit

A Time-stamping Unit is the composition of

- A time stamping context, directly managed by the TOE;
- A key pair, stored within the HSM, outside of the TOE.

4.2.3 TOE Environment general overview

The TOE by itself is not able to ensure the complete security of the time stamping generation process and shall be operated in an environment that meets the requirement described in this document.

More generally, this PP has been written for Trusted Service Provider operating time-stamping authority to help them to meet the requirements of the [EN319421] or equivalent. Therefore, the TOE shall be operated in an environment that is compliant with the above technical specification and, particularly, with a Hardware Security Module that shall meet the requirement of [EN319421] or equivalent.

The following figure presents the general overview of the expected TOE environment.

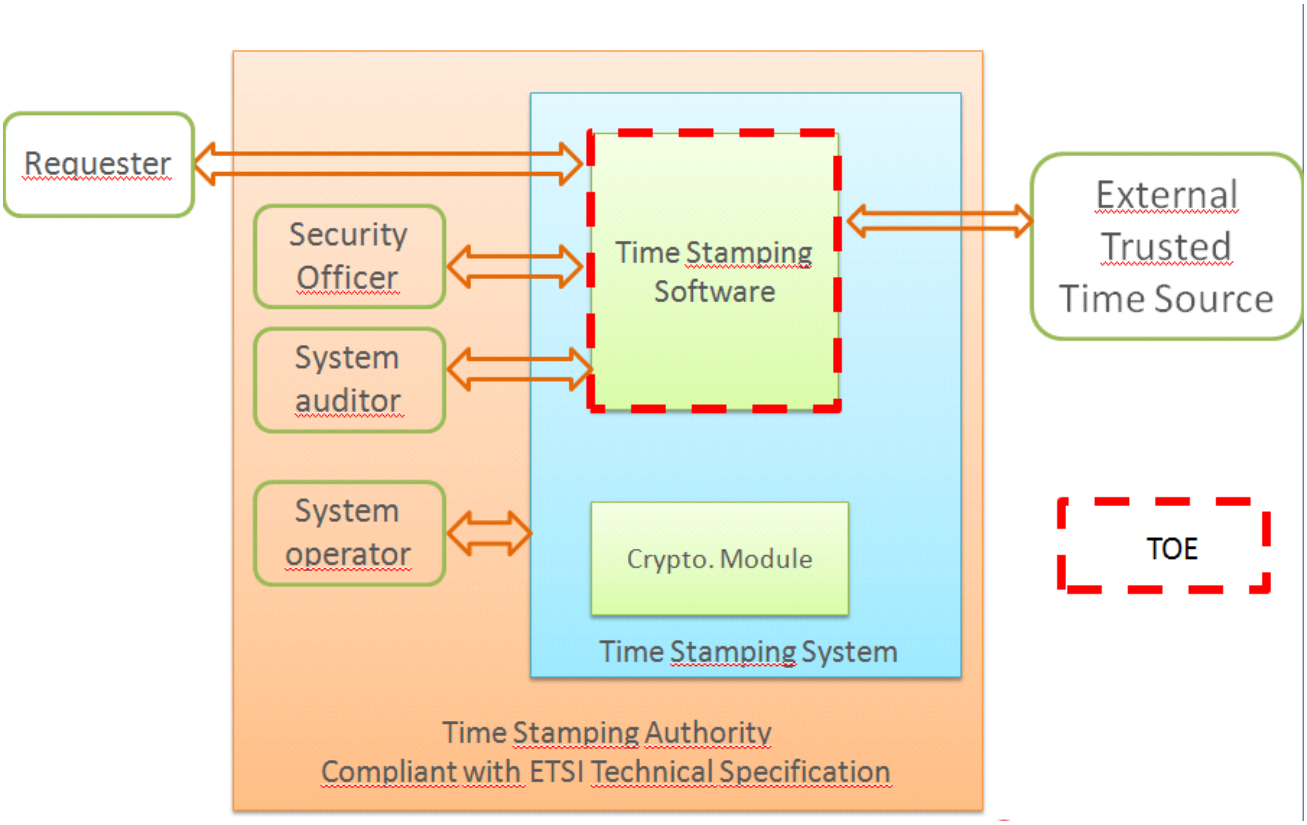

Figure 5: Interactions of the TOE with its environment

The TOE and Time-stamping system, including the crypto-module, are intended to be operated a Time Stamping Authority. The Security Officer, the System auditor and the System Operator are located within the perimeter of the TSA Authority and are considered as Trusted Roles. The requester is not part of the Time-stamping authority but is in relation with the Time-stamping authority as a consumer of the Time-stamping service.

4.2.4 Required non-TOE hardware/software/firmware

The TOE needs, at least, the following hardware/software/firmware to operate:

- A server running a general purpose operating system, and is part of the Time Stamping System.
- A Cryptographic module, able to create digital signatures of the time-stamp tokens, and is part of the Time Stamping System.
- An external reference Clock

The Crytpographic module shall be hardware based and that shall meet the requirements of:

- o [EN319421] §7.5.2 or equivalent; or
- o identified in ISO/IEC 19790, level 3 or higher; or

  NOTE : Demonstrated conformance to FIPS PUB 140-2 , level 3 is considered as fulfilment of this requirement.

- o identified in [CEN TS 419 221-2] or [CEN TS 419 221-4] or [CEN TS 419 221-5]; or
- o of a trustworthy system which is assured to EAL 4 or higher in accordance to ISO/IEC 15408, or equivalent security criteria. This shall be to a security target or protection profile which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures.

The external reference Clock that is synchronized with UTC time such that

- o The time values the TSU uses in the time-stamp token shall be traceable to at least one of the real time values distributed by a UTC(k) laboratory.
- o The time included in the time-stamp token shall be synchronized with UTC within the accuracy defined in the policy and, if present, within the accuracy defined in the time-stamp token itself.

It is strictly forbidden to use non-TOE software to implement TSF-enforcing functionalities. All TSF-enforcing functions handled by software shall be included within the TOE. For example, external libraries may be used for cryptographic computation as long as these libraries are included in the TOE scope. The TOE may use features of the HSM, as long as these features are within the scope of the HSM Security Target, have been evaluated at least at the same EAL level than the TOE and are implemented according to the HSM guidance (*i.e.* in CC evaluated mode).

5 Conformance claims

5.1 CC conformance claim

This Protection Profile (PP) complies with Common Criteria, version 3.1, revision 4, September 2012, for both the content and presentation requirements.

All functional and assurance security requirements laid out in this PP comply with Part 2 and Part 3 respectively of the aforementioned Common Criteria version.

This PP is conforming to assurance package Evaluation Assurance Level 4 augmented (EAL4+) as defined in Part 3 of the aforementioned Common Criteria version. Augmentation results from the selection of:

- ALC_FLR.3 Systematic flaw remediation

5.2 PP claim

This PP does not claim conformance to any other PP.

5.3 Conformance rationale

This PP does not provide a conformance rationale because it does not claim conformance to any other PP.

5.4 Conformance statement

The PP requires demonstrable conformance of the ST or PP claiming conformance to this PP.

6 Security problem definition

6.1 TOE assets

The TOE implements services that include user management, TSU configuration, start of TSU operation, stop of TSU operation if the clock is detected as being out of the stated accuracy, key destruction, generation of key pair, public key export for certificate request, certificate import, timestamp token generation and internal audit.

The primary assets that need to be protected by the TOE are the following TOE internal data:

- **R.REQUEST**. This asset is the time-stamping request sent by the requester to the TOE in order to obtain a time-stamp. This request shall contain:
    - the hash of the document to be processed,
    - identification of the hash algorithm used to calculate the hash of the document,

  Other information may be included in R.REQUEST.

  It is important to notice that the request contains the hash of the document obtained with the hash algorithm defined in the request and not the document itself.

  R.REQUEST shall be protected in integrity when inside the TOE.

- **R.TIMESTAMP_TOKEN**. The time-stamp token is a signed electronic message associating a document hash with a UTC time and a unique reference to the time-stamping policy. Other information may be included. The time-stamp is generated based on the time-stamp request information and signed using the active private key of the time stamping context of the TSU.

  R.TIMESTAMP_TOKEN shall be protected in integrity and its origin shall be authenticated.

- **R.CONTEXT**. The time-stamp context comprises all the information needed to operate a TSU. This asset contains the following elements:
    - The identification of the time source to be used when the TOE manages multiple time source references;
    - The accuracy of the time in the time-stamp tokens with respect to UTC.
    - The configuration of the supported time-stamping policies. For each supported policy, the time-stamp context contains:
        - The identifier of the time-stamping policy;
        - The identifier(s) of the supported hash algorithm(s);
    - The identification of the default time-stamping policy;
    - The identifier(s) of the key pair(s) to be used;
    - The certificate of the TSU public key. This certificate is issued by a certification authority, and it is included when the context state is in operational mode. The public key value within the certificate shall be the same as the public key of the key pair identified in the context.

  R.CONTEXT shall be protected in integrity.

- **R.DATE_AND_TIME**. This asset provides the date and time (reference time) to be included in each time-stamp token. Associated with this date and time is:

- A synchronisation state (internal clock manager), that indicates whether the clock is synchronized with UTC or not.
- A synchronization precision value.

R.DATE_AND_TIME shall be protected in integrity.

- **R.KEY_PAIR_PUB**. This asset is the public key of a time-stamping context. The public key can be used by the requester and third parties to verify the integrity and authorship of the signed time-stamp.

  R.KEY_PAIR_PUB shall be protected in integrity prior to being certified.

- **R.KEY_PAIR_PRIV**. This asset is the handler of or reference to the private key of a time-stamping context. The private key, stored in the cryptographic module, is used by the TSU to digitally sign the time-stamps.

  R.KEY_PAIR_PRIV shall be protected in integrity and confidentiality.

  Note: The private key itself shall be protected in integrity and in confidentiality by the cryptographic module.

- **R.TSF_DATA**: TSF data, including:
  - Authentication data of TOE users (administrators and auditors), which shall be protected in confidentiality and integrity.
  - Non-confidential user/role related data (identifier, access control lists, role definitions, etc.). These data shall be protected in integrity.

- **R.AUDIT_DATA**. Internal audit records and that shall be protected in integrity.

Next table correlates the TOE internal data types explained above with those data types considered in the formalisation of the security functional requirements (SFR):

TOE internal data type	SFR-related data type
R.REQUEST	User data[1]
R.TIMESTAMP_TOKEN	
R.CONTEXT	
R.DATE_AND_TIME	
R.KEY_PAIR_PUB	
R.KEY_PAIR_PRIV	
R.AUDIT_DATA	
R. TSF_DATA	TSF data[2]

[1] data for the user that does not affect the operation of the TSF (TOE Security Functionality). For example, in the case of R.AUDIT_DATA, the audit records generated internally in the TOE are intended to be revised by the Auditor.

[2] data for the operation of the TOE upon which the enforcement of the SFR relies.

6.2 Threats

The expected attackers are qualified so as to have Enhanced-Basic attack potential, in accordance with the security assurance given by AVA_VAN.3 Focused vulnerability analysis.

The expected threat agents are:

- **TA.EXTERNAL**

  This agent represents an entity that does not hold any authorised role to operate or interact with the TOE. This agent may operate through the remote or local interfaces of the TOE, or even have direct physical access to the TOE. Examples of this threat agent are: unauthorised TOE personnel, cybercriminals, and hackers in general.

- **TA.INSIDER**

  This agent represents an entity that holds an authorised role to operate or interact with the TOE, and which has the intention to compromise the TOE assets. This agent may operate through the remote or local interfaces of the TOE, or even have direct physical access to the TOE. Examples of this threat agent are: auditors and administrators, such as the system administrator.

- **TA.INADVERTENT**

  This agent represents an entity that holds an authorised role to operate or interact with the TOE, but which does not have the intention to compromise the TOE assets. This agent may operate through the remote or local interfaces of the TOE, or even have direct physical access to the TOE. Examples of this threat agent are: auditors and administrators.

The expected threats to the TOE may be:

- **T.CONTEXT_ALTERATION**

  A TA.INSIDER or TA.INADVERTENT might change the operational time-stamping context (R.CONTEXT) with the purpose to or with the consequence of using a context with weaker security attributes (e.g. weak hash algorithms), a compromised private key for which the certificate revocation has not been processed yet, etc.

- **T.DATE_AND_TIME_ALTERATION**

  A TA.INSIDER might change the reference date and time and/or the synchronisation state of R.DATE_AND_TIME with the purpose to make the TOE issue signed time-stamps with an intended time that deviates from the actual UTC date and time. The threat can be materialised in two ways:

  (1) The TA.INSIDER sets the time of the internal clock with an arbitrary date in the past or in the future that is outside the range of clock accuracy.

  (2) The TA.INSIDER sets the time of the internal clock with an arbitrary date in the past or in the future that is inside the range of clock accuracy, and performs this attack over again until a gap greater than the the range of the clock accuracy is reached.

- **T.PRIVATE_KEY_ALTERATION**

  A TA.EXTERNAL or a TA.INSIDER might modify or alter the R.KEY_PAIR_PRIV while being operated inside the TSU, resulting in a loss of integrity and/or availability of the R.KEY_PAIR_PRIV.

  For instance, a TA.INSIDER such a malicious auditor without authorisation to change the R.KEY_PAIR_PRIV reference to another private key that may not be stored in a HSM or that may produce non verifiable timestamps.

- **T.PUBLIC_KEY_ALTERATION**

  A TA.EXTERNAL or a TA.INSIDER might modify or alter the R.KEY_PAIR_PUB before creating the certificate request for further export, resulting in a loss of integrity of the R.KEY_PAIR_PUB.

- **T.PRIVATE_KEY_DERIVATION**

  A TA.EXTERNAL or a TA.INSIDER might derive all or parts of private key referred by R.KEY_PAIR_PRIV using knowledge gained about, for example, the corresponding public key, the cryptosystem and the key generation process. This knowledge might enable the attacker to conduct certain cryptanalysis attacks that does not require access to the environment where the private key is stored.

  Notice that the private key referred by R.KEY_PAIR_PRIV is intended to be stored in the HSM outside the perimeter of the TOE. Therefore, this threat apply mainly on the private key referred by R.KEY_PAIR_PRIV and not on R.KEY_PAIR_PRIV itself. However, this threat applies in the case where R.KEY_PAIR_PRIV refers to a private key generated with a weak algorithm.

- **T.PRIVATE_KEY_DISCLOSURE**

  A TA.EXTERNAL or a TA.INSIDER might disclose all or part of private key referred by R.KEY_PAIR_PRIV over logical TOE interface or physical interface of the operational environment by using covert channel mechanisms.

  Notice that the private key referred by R.KEY_PAIR_PRIV is intended to be stored in the HSM outside the perimeter of the TOE. Therefore, this threat apply mainly on the private key referred by R.KEY_PAIR_PRIV and not on R.KEY_PAIR_PRIV itself. However, this threat applies in the case where R.KEY_PAIR_PRIV refers to a private key generated with a weak algorithm.

- **T.CRYPTO**

  A TA.EXTERNAL or a TA.INSIDER might deduce the R.KEY_PAIR_PRIV from the R.KEY_PAIR_PUB or create a forged digital signature due to the use of a weak cryptographic suite by TOE for either key pair generation or digital signature operation.

- **T.MISUSE**

  A TA.EXTERNAL, TA.INSIDER or a TA.INADVERTENT, who has access to the TOE services, uses these services without proper authorisation or in a manner for which they are not intended, having an impact on the R.REQUEST, R.TIMESTAMP_TOKEN, R.CONTEXT, R.DATE_AND_TIME, R.KEY_PAIR_PUB, R.KEY_PAIR_PRIV, R.AUDIT_DATA or R.TSF_DATA.

  For instance, a TA.INSIDER such a malicious auditor without authorisation to generate key pairs (R.KEY_PAIR_PUB and R.KEY_PAIR_PRIV) may misuse the TOE services to do so.

- **T.INSECURE_INITIALISATION**

  A TA.EXTERNAL, a TA.INSIDER or a TA.INADVERTENT might initialise the TOE with insecure R.TSF_DATA.

- **T.AUDIT_ALTERATION**

  A TA.EXTERNAL or TA.INSIDER might alter the TOE R.AUDIT_DATA.

6.2.1 Relation between threats and assets

Asset	Security dimension(s)	Threat(s)
R.REQUEST	Integrity	T.MISUSE
R.TIMESTAMP_TOKEN	Integrity	T.MISUSE
	Origin authentication	T.MISUSE
R.CONTEXT	Integrity	T.CONTEXT_ALTERATION T.MISUSE
R.DATE_AND_TIME	Integrity	T.DATE_AND_TIME_ALTERATION T.MISUSE
R.KEY_PAIR_PUB	Integrity	T.PUBLIC_KEY_ALTERATION T.MISUSE T.MALWARE_INJECTION
R.KEY_PAIR_PRIV	Confidentiality	T.PRIVATE_KEY_DERIVATION T.PRIVATE_KEY_DISCLOSURE T.MISUSE T.CRYPTO
	Integrity	T.PRIVATE_KEY_ALTERATION T.MISUSE
R.TSF_DATA (Authentication data)	Confidentiality	T.MISUSE
	Integrity	T.MISUSE
R.TSF_DATA (non-confidential data)	Integrity	T.MISUSE T.INSECURE_INITIALISATION
R.AUDIT_DATA	Integrity	T.MISUSE T.AUDIT_ALTERATION

6.3 Organisational security policies

- **OSP.ALGORITHMS**

  Only approved algorithms and algorithm parameters defined as acceptable for being used in R.KEY_PAIR_PUB/R.KEY_PAIR_PRIV pair generation and time-stamps signing shall be used by the TOE. This includes the generation of random numbers and the quality of the R.KEY_PAIR_PUB/R.KEY_PAIR_PRIV pairs generated.

  Approved algorithms and algorithm parameters defined as acceptable shall be used to ensure the confidentiality and integrity of private key referred by R.KEY_PAIR_PRIV, and the integrity of R.KEY_PAIR_PUB.

  The TOE shall support cryptographic algorithms and key lengths conformant to the rules defined by the relevant national CC Certification Body.

Note: See ETSI TS 119 312 [ETSI 119 312] and [SOG-IS-Crypto] for guidance on signature algorithms and their parameters.

Application note: The PP/ST writer should ensure that the algorithms and algorithms parameters specified in the PP/ST conform to the rules and recommendations defined by the national authority.

- **OSP.SERVICE**

The TOE shall generate timestamps in conformity with the time-stamping policy. Time-stamps shall be signed using the private key referenced in the R.CONTEXT.

- **OSP.REQUEST_MGMT**

  The time-stamping protocol implemented by the TOE shall ensure that the time-stamp R.TIMESTAMP_TOKEN is generated in conformity with the data received in the request R.REQUEST.

- **OSP.CLOCK**

  During the initialisation of the TSU, the reference time of the R.DATE_AND_TIME shall be checked to ascertain that it is synchronised with a trusted external UTC time source.

6.4 Assumptions

- **A.TSS**

  The Time Stamping System meets the requirements laid down in [EN319421] or equivalent. In addition, the communication network where the TOE operates is secured to prevent intrusions and other forms of cyber-attacks. The operational environment also implements a secure communication channel, such as HTTPs or similar, to protect the confidentiality and integrity of the information exchanged between the TOE and external entities.

- **A.ACCESS_PROTECTED**

  The TOE is protected by physical and organisational protection measures implemented by the TOE environment. Those measures shall restrict the TOE physical access (e.g. for administration purposes) to authorised persons only and shall require dual control. These measures counteract threats that might try to physically manipulate the TOE operational environment with the intent to:

  - derive all or part of the private key referred by R.KEY_PAIR_PRIV (by side channel for example), and/or
  - alter received R.REQUEST, generated R.TIMESTAMP_TOKEN, R.CONTEXT, R.DATE_AND_TIME, R.KEY_PAIR_PUB, R.KEY_PAIR_PRIV, R.AUDIT_DATA or R.TSF_DATA, and/or
  - make R.KEY_PAIR_PRIV, R.TSF_DATA (VAD or RAD) or R.AUDIT_DATA unavailable, and/or
  - destroy the TOE by deliberate action.

- **A.REF_TIME**

  It is assumed that no attack can simultaneously compromise the reference time and the TOE clock checking mechanism, e.g., by changing the synchronization state.

  It is supposed that it will be processed, during the time-stamping unit initialization, to a verification of a correct initialization of the time reference.

  Moreover it is supposed than no attack can compromise simultaneously and in a coherent way the values of a time-stamping unit internal clock and the time reference.

  Application note

  As mentioned in section 4.2.3, the TOE is intended to be operated by a Trusted Service Provider operating time-stamping authority. Therefore, the TOE is intended to be operated in a secured environment that meet the requirements of the [EN319421] and provide appropriate security measures to limit simultaneous attacks

on the time reference and the TOE clock checking mechanism. On top of these requirement, we provide the following recommendations to meet the assumption.

The initialization of the time reference must include, if applicable, the verification of the wires between the time-stamping unit and the external sources. In the case of radio sources, this verification must also include the wires to the antennas.

The time reference can be obtained from several manners, for example with the assistance:

- of an authenticated single external source,
- of not authenticated multiple external sources,
- of an atomic clock located in the monitoring environment of the time-stamping system.

The risk of a simultaneous compromising and in a coherent way of the values of the time-stamping unit internal clock and of the time reference can for example be limited by:

- the choice of different technologies (in particular when an atomic clock provides the time reference, it should not also make function of internal clock),
- the selection of different locations.

- **A.TIMESTAMP_VERIFICATION**

The requester verifies the correctness of the time-stamps received from the TOE and ensures its preservation, if needed. For that, the requester:

- Verifies the digital signature of the time-stamp.
- Checks if the hash within the received time-stamp is the same as the one included in the corresponding request sent to the TOE.

- **A.AUDIT_REVIEW**

TOE Auditors check the audit trails on a regular basis, and notify the corresponding authority in the case that an incident occurred.

- **A.CA**

The Certification Authority that issues the certificates to the TOE implements a set of practices in conformity with their CP/CPS.

- **A.CERTIFIED_CM**

The cryptographic module used by the TOE to digitally sign the time-stamps is a certified device that meets:

- o the requirements of [EN319421]§7.5.2 or equivalent.
- o or the following:
  - meets the requirements identified in ISO/IEC 19790, level 3 or higher;

  NOTE : Demonstrated conformance to FIPS PUB 140-2 , level 3 is considered as fulfilment of this requirement.

  - meets the requirements identified in [CEN TS 419 221-2] or [CEN TS 419 221-4] or [CEN TS 419 221-5]; or

- is a trustworthy system which is assured to EAL 4 or higher in accordance to ISO/IEC 15408, or equivalent security criteria. This shall be to a security target or protection profile which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures.

- **A.SECURE_BACKUP**

  If the cryptographic module used by the TOE allows backup of TSU private keys, they are copied, stored and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment (see A.ACCESS_PROTECTED). The personnel authorised to carry out this function are limited to those requiring to do so under the established practices.

  Any backup copies of the TSU private signing keys are protected by the cryptographic module to ensure its integrity and confidentiality before being stored outside that device.

  After expiration of the certificate associated to the private key, all backups of the key is destroyed or made unable to be used by appropriate means.

7 Security objectives

This section identifies and defines the security objectives for the TOE and its environment. Security objectives reflect the stated intent to counter the identified threats, as well as comply with the identified organisational security policies and assumptions.

7.1 Security objectives for the TOE

- **O.AUDIT** Generation and Export of Audit Data

  The TOE shall audit the following events:

  - TOE initialisation
  - TOE start-up
  - Start of TSU operation
  - Stop of TSU operation
  - Desynchronisation of the TOE
  - Generation of R.KEY_PAIR_PUB/ R. KEY_PAIR_PRIV pairs
  - Export of R.KEY_PAIR_PUB for certificate request
  - Certificate import
  - Changes in the R.CONTEXT, including changes in the time source to use, supported time-stamping policies, identification of the default time-stamping policy, the identifier of the default time-stamping policy, the identifier(s) of the key pair(s) to be used, and the certificate of the TSU public key.
  - Updates of the internal clock values, including the date, time and the synchronisation state.
  - Destruction of R.KEY_PAIR_PUB/ R. KEY_PAIR_PRIV pairs
  - Time-stamp generation
  - Unsuccessful authentication
  - Modification of TOE user management data
  - Adding new users or roles
  - Deleting users or roles
  - Exporting and deleting audit trail records

  The audit data shall associate each auditable event with the identity of the user that caused the event. For the time-stamp generation event, the audit data shall incorporate the identification of the time source, the time-stamping policy and the identifier of the key pair used in the process. The integrity of the audit trail shall be ensured. The TOE shall export the audit data upon request of the Auditor. The TOE shall provide the management function for the audit to the Auditor only.

- **O.USER_AUTHENTICATION** Authentication of TOE Users

  The TOE shall be able to identify and authenticate the users acting with a defined role, before allowing any access to TOE protected assets (TOE services – except time-stamp generation service, for which no

authentication is needed – and TOE internal data). Identification and authentication shall be based on user identity.

- **O.RBAC** Role-based Access Control to TOE Services

  The TOE shall restrict the access to its assets (TOE services – except time-stamp generation service, for which no access control is needed – and TOE internal data) depending on the user role, allowing user access only to those services and data explicitly authorised to the assigned role. Assignment of services to roles shall be done either by explicit action of an Administrator or by default.

- **O.PUBLIC_KEY_MANAGEMENT** Secure Management of Public Key

  The TOE shall check the integrity of the R.KEY_PAIR_PUB when it is under the control of the TOE and before it is exported for certification.

- **O.SYNCHRONISATION** Stop of operation under asynchrony with UTC time source

  The TOE shall stop issuing timestamps if the internal clock is out of the specified accuracy.

- **O.AUDIT_PROTECTION** Protection of audit data

  The TOE shall implement mechanisms to prevent a T.EXTERNAL and T.INSIDER from modifying R.AUDIT_DATA.

- **O.CRYPTO** Secure Cryptographic Operations

  Only approved algorithms and algorithm parameters defined as acceptable for being used in R.KEY_PAIR_PUB/R.KEY_PAIR_PRIV pair generation and time-stamps signing shall be used by the TOE.

  The TOE shall support cryptographic algorithms and key lengths conformant to the rules defined by the relevant national CC Certification Body.

7.2 Security objectives for the operational environment

The following security objectives relate to the TOE environment. This includes the rest of the Time Stamping System (Operating System, Drivers, HW and TSU) as well as the procedures for the secure operation of the TOE.

- **OE.TSS** Time Stamping System

  The Time Stamping System shall meet the requirements laid down in [EN319421] or equivalent. In addition, the communication network where the TOE operates shall be secured to prevent intrusions and other forms of cyber-attacks. The operational environment shall also implement a secure communication channel, such as HTTPs or similar, to protect the confidentiality and integrity of the information exchanged between the TOE and external entities.

- **OE.KEY_PAIR_GENERATION** Public Key/Private Key Pair Generation

  For the R.KEY_PAIR_PUB / R.KEY_PAIR_PRIV pair generation, the TOE environment shall implement secure cryptographic algorithms and parameters compliant with the requirements established by the national authority.

Note: See ETSI TS 119 312 [ETSI 119 312] and [SOG-IS-Crypto] for guidance on signature algorithms and their parameters.

- **OE.PRIVATE_KEY_MANAGEMENT** Secure Management of Private Key

The TOE environment shall ensure the confidentiality and integrity of the private key referred by R.KEY_PAIR_PRIV. This includes protection against disclosing completely or partly the private key referred by R.KEY_PAIR_PRIV in clear through any logical interface. For confidentiality and integrity purposes, the TOE environment shall also implement secure cryptographic algorithms and parameters compliant with the requirements established by the national authority.

- **OE.PROTECT_ACCESS** Prevention of Unauthorised Physical Access

  The TOE shall be protected by physical, logical and organisational protection measures implemented by the TOE environment in order to prevent any TOE modification, as well as any protected assets disclosure. Those measures shall restrict the TOE usage and access to authorised persons only and shall require dual control. The TOE operational environment shall follow the policy requirements established in in [EN319421].

- **OE.PERSONNEL** Liability and Training

  The personnel that have access to the TOE or use its services shall be aware of civil, financial and legal responsibilities, as well as the obligations they have to face, depending on their role. The personnel shall be trained on correct usage of the TOE.

- **OE.SECURE_INIT** Secure Initialisation Procedures

  Procedures and controls in the TOE environment shall be defined and applied to permit the secure set-up and initialisation of the TOE services within a TSP system in compliance with the requirements of the EU directive and the Policy for certification authorities issuing qualified certificates [8]. This includes the initial configuration of R.TSF_DATA, as well as TSU configuration and the start of TSU operation by the security officer. During the initialisation of the TSU, the security officer shall check that the reference time of the R.DATE_AND_TIME is synchronised with a trusted external UTC time source.

  Moreover, the TOE environment shall guarantee that no attack can compromise simultaneously and in a coherent way the value of the reference time and the synchronisation state. This can be achieved by, for example:

  - Selecting different technologies (e.g. for the atomic clock, if used as the time reference in the TOE environment)

  - Selecting different locations, if the time reference is calculated based on the values provided by more than one external source which the TOE is connected to.

- **OE.SECURE_OPER** Secure Operating Procedures

  Procedures and controls in the TOE environment shall be defined and applied to permit the secure operation of the TOE services within a TSP system in compliance with the requirements of the Regulation (EU) n.910/2014 and the Policy for certification authorities issuing qualified certificates [8].

- **OE.TIMESTAMP_VERIFICATION** Time-stamp verification

  The requester shall verify the correctness of the time-stamps received from the TOE and ensure its preservation, if needed. For that, the requester shall:

  - Verify the digital signature of the time-stamp.

  - Check if the hash within the received time-stamp is the same as the one included in the corresponding request sent to the TOE.

- **OE.AUDIT_REVIEW** Audit review

  TOE Auditors shall check the audit trails on a regular basis, and notify the corresponding authority in the case that an incident occurred.

- **OE.CA** Certification Authority

  The Certification Authority that issues the certificates to the TOE shall implement a set of practices in conformity with their CP/CPS.

Note: See ETSI EN 319 411-2 [ETSI 319 411-2] Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing

EU qualified certificates .

- **OE.CERTIFIED_CM** Certified cryptographic module

  The cryptographic module used by the TOE to digitally sign the time-stamps shall be a certified device that meets:

  - the requirements of [EN319421]§7.5.2 or equivalent.
  - or the following:
    - meets the requirements identified in ISO/IEC 19790, level 3 or higher;

    NOTE : Demonstrated conformance to FIPS PUB 140-2 , level 3 is considered as fulfilment of this requirement.

    - meets the requirements identified in [CEN TS 419 221-2] or [CEN TS 419 221-4] or [CEN TS 419 221-5]; or
    - is a trustworthy system which is assured to EAL 4 or higher in accordance to ISO/IEC 15408, or equivalent security criteria. This shall be to a security target or protection profile which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures.

- **OE.SECURE_BACKUP Secure backup of private keys**

  If the cryptographic module used by the TOE allows backup of TSU private keys, they shall be copied, stored and recovered only by personnel in trusted roles (see OE.PERSONNEL) using, at least, dual control in a physically secured environment (see OE.PROTECT_ACCESS). The personnel authorised to carry out this function shall be limited to those required to do so under the established practices.

  Any backup copies of the TSU private signing keys shall be protected by the cryptographic module to ensure its integrity and confidentiality before being stored outside that device. After expiration of the certificate associated to the private key, all backups of the key shall be destroyed or made unable to be used by appropriate means.

7.3 Security objectives rationale

The following table shows the correspondence between the security objectives applicable to the TOE and the environment and the countered threats, the assumptions and the organizational security policies.

	T.CONTEXT_ALTERATION	T.DATE_AND_TIME_ALTERATION	T.PRIVATE_KEY_ALTERATION	T.PUBLIC_KEY_ALTERATION	T.PRIVATE_KEY_DERIVATION	T.PRIVATE_KEY_DISCLOSURE	T.CRYPTO	T.MISUSE	T.INSECURE_INITIALISATION	T.AUDIT_ALTERATION	OSP-ALGORITHMS	OSP.SERVICE	OSP.REQUEST_MGMT	OSP.CLOCK	A.TSS	A.ACCESS_PROTECTED	A.REF_TIME	A.TIMESTAMP_VERIFICATION	A.AUDIT_REVIEW	A.CA	A.CERTIFIED_CM	A.SECURE_BACKUP
O.AUDIT	X	X	X	X				X	X			X										
O.USER_AUTHENTICATION			X	X				X														
O.RBAC			X	X				X														
O.CRYPTO					X		X				X											
O.PUBLIC_KEY_MANAGEMENT				X							X											
O.SYNCHRONISATION		X																				
O.AUDIT_PROTECTION										X												
OE.TSS								X							X							
OE.KEY_PAIR_GENERATION					X						X											
OE.PRIVATE_KEY_ MANAGEMENT			X			X					X											
OE.PROTECT_ACCESS						X										X						
OE.PERSONNEL	X	X	X	X		X		X	X													
OE.SECURE_INIT									X					X			X					
OE.SECURE_OPER						X		X														
OE.TIMESTAMP_VERIFICATION													X					X				
OE.AUDIT_REVIEW	X	X	X	X				X	X			X							X			
OE.CA																				X		
OE.CERTIFIED_CM						X															X	
OE.SECURE_BACKUP			X			X																X

Security objectives coverage is met as each threat, assumption and organizational security policy is addressed by at least one security objective, and every security objective is mapped with at least one threat, assumption or organizational security policy.

Next, the rationale for each matching is provided:

T.CONTEXT_ALTERATION is a threat by which a TA.INSIDER or TA.INADVERTENT changes the operational time-stamping context (R.CONTEXT) with the purpose to or with the consequence of using a context with weaker security attributes (e.g. weak hash algorithms), a compromised private key for which the certificate revocation has not been processed yet, etc. This threat is countered by **O.AUDIT** (Generation and Export of Audit Data), which establishes the need to record events relevant to changes in the context, and **OE.AUDIT_REVIEW** (Audit review), which ensures that the auditors regularly check the audit trails and notify in the case that an incident occurs. Finally, this threat is diminished by **OE.PERSONNEL** (Liability and Training), which covers the awareness and training of the personnel that use the TOE. This objective diminishes the threat in both cases (TA.INSIDER or TA.INADVERTENT) due to the liability issues, and also in the case of a TA.INADVERTENT because of the training undertaken.

T.DATE_AND_TIME_ALTERATION is a threat that represents a TA.INSIDER that changes some information of R.DATE_AND_TIME with the purpose to make the TOE issue signed time-stamps with an intended time that deviates from the actual UTC date and time. The threat details two possible ways of implementing the attack, both of which are meant at modifying the reference time with an arbitrary date. This threat is countered by **O.AUDIT** (Generation and Export of Audit Data), which establishes the need to record events relevant to changes in the values managed by the internal clock, and **OE.AUDIT_REVIEW** (Audit review), which ensures that the auditors regularly check the audit trails and notify in the case that an incident occurs. This threat is diminished by **OE.PERSONNEL** (Liability and Training), reducing the motivation to execute the adverse action due to the liability and legal consequences. Finally, this threat is mitigated by **O.SYNCHRONISATION** (Stop of operation under asynchrony with UTC time source), by which no timestamp is issued if the synchronisation to the trusted UTC time source is outside the specified limit. This security objective mitigates one of two possible implementation ways of the threat. In particular, case (1), when the TA.INSIDER sets the time of the internal clock with an arbitrary date in the past or in the future that is outside the range of clock accuracy.

T.PRIVATE_KEY_ALTERATION is a threat where a TA.EXTERNAL or a TA.INSIDER modifies or alters the private key while being operated inside the TSU, resulting in a loss of integrity and/or availability of the private key. This threat is countered by several security objectives. First, audit trails related to changes in the private key (Generation of R.KEY_PAIR_PUB/ R. KEY_PAIR_PRIV pairs, Destruction of R.KEY_PAIR_PUB/ R. KEY_PAIR_PRIV pairs) are recorded by the TOE (**O.AUDIT** (Generation and Export of Audit Data)) and later on reviewed by the auditors (**OE.AUDIT_REVIEW** (Audit review)). This ensures that if any adverse action towards changing the private key occurs, in particular those that trigger either of these two events, then the necessary information is recorded to trace back to the corresponding user and date. This is relevant for TA.INSIDER threat agent, who shall be authenticated in the TOE. For threat agents TA.EXTERNAL, this threat is countered by authentication and access control mechanisms implemented by the TOE, and represented by the objectives **O.USER_AUTHENTICATION** (Authentication of TOE Users) and **O.RBAC** (Role-based Access Control to TOE Services) respectively. This threat is also countered by **OE.PRIVATE_KEY_MANAGEMENT** (Secure Management of Private Key), by which the TOE environment has to ensure the confidentiality and integrity of the private key. Also, for confidentiality and integrity purposes, the TOE environment has to implement secure cryptographic algorithms and parameters compliant with the requirements established by the national authority. This threat is also diminished by **OE.PERSONNEL** (Liability and Training) due to the liability issues involved. Finally, the impact derived from this threat is mitigated by a secure backup of TSU private keys during which the cryptographic module preserves the integrity and confidentiality of the keys, if the cryptographic module used by the TOE permits the backup operation (**OE.SECURE_BACKUP** (Secure backup of private keys)). By having a backup of the private key the TOE is able to restore it to a previous (valid) value if the alteration is detected.

T.PUBLIC_KEY_ALTERATION is a threat where a TA.EXTERNAL or a TA.INSIDER modifies or alters the public key before creating the certificate request for further export, resulting in a loss of integrity of the public key. This threat is countered by several security objectives. First, audit trails related to changes in the public key (Generation of R.KEY_PAIR_PUB/ R. KEY_PAIR_PRIV pairs, Destruction of R.KEY_PAIR_PUB/ R. KEY_PAIR_PRIV pairs) and export of the public key (Export of R.KEY_PAIR_PUB for certificate request) are recorded by the TOE (**O.AUDIT** (Generation and Export of Audit Data)) and later on reviewed by the auditors (**OE.AUDIT_REVIEW** (Audit review)). This ensures that if any adverse action towards changing the public key occurs, in particular those that trigger either of these two events, then the necessary information is recorded to trace back to the corresponding user and date. This is relevant for TA.INSIDER threat agent, who shall be authenticated in the TOE. For threat agents TA.EXTERNAL, this threat is countered by authentication and

access control mechanisms implemented by the TOE, and represented by the objectives **O.USER_AUTHENTICATION** (Authentication of TOE Users) and **O.RBAC** (Role-based Access Control to TOE Services) respectively. This threat is also countered by **O.PUBLIC_KEY_MANAGEMENT** (Secure Management of Public Key), by which the TOE ensures the integrity of the public key when it is under the control of the TOE and before it is exported for certification. Finally, this threat is diminished by **OE.PERSONNEL** (Liability and Training) due to the liability issues involved.

T.PRIVATE_KEY_DERIVATION is a threat by which a TA.EXTERNAL or a TA.INSIDER derives all or parts of the private key using knowledge gained about, for example, the corresponding public key, the cryptosystem and the key generation process. This knowledge might enable the attacker to conduct certain cryptanalysis attacks that does not require access to the environment where the private key is stored.. This threat is countered by two security objectives. First, **OE.KEY_PAIR_GENERATION** (Public Key/Private Key Pair Generation) states that the TOE environment has to implement secure cryptographic algorithms and parameters compliant with the requirements established by the national authority to be used for the key pair generation. Second, this threat is counteracted by **O.CRYPTO** (Secure Cryptographic Operations), by which only strong approved algorithms and algorithm parameters defined as acceptable for being used in R.KEY_PAIR_PUB/R.KEY_PAIR_PRIV pair generation and time-stamps signing shall be used by the TOE.

T.PRIVATE_KEY_DISCLOSURE is a threat where a TA.EXTERNAL or a TA.INSIDER discloses all or part of the private key over logical TOE interface or physical interface of the operational environment by using covert channel mechanisms. This threat is countered by several security objectives. **OE.PRIVATE_KEY_MANAGEMENT** (Secure Management of Private Key) establishes that the TOE environment has to ensure the confidentiality and integrity of the private key. Also, for confidentiality and integrity purposes, the TOE environment has to implement secure cryptographic algorithms and parameters compliant with the requirements established by the national authority. In addition, the use of a certified cryptographic module (**OE.CERTIFIED_CM** (Certified cryptographic module)) provides a minimum level of assurance regarding the protection of the private key, diminishing the possibility of an attacker to export the private key from the module. On the other hand, **OE.SECURE_OPER** (Secure Operating Procedures) establishes procedures and controls in the TOE environment to ensure the secure operation of the TOE services, diminishing the possibility of an attacker to implement the adverse action. The physical access to the TOE (**OE.PROTECT_ACCESS** (Prevention of Unauthorised Physical Access)) is also restricted to authorised personnel only, eliminating the possibility of a TA.EXTERNAL to use physical interfaces for the private key disclosure. In the case the cryptographic module used by the TOE supports backup of TSU private keys, confidentiality of the private key is ensured by **OE.SECURE_BACKUP** (Secure backup of private keys), aimed at establishing personnel, procedurals and technical measures during copy, storage and restoration of private keys. Finally, this threat is diminished by **OE.PERSONNEL** (Liability and Training) due to the liability issues involved.

T.CRYPTO is a threat where a TA.EXTERNAL or a TA.INSIDER might deduce the private key referred by R.KEY_PAIR_PRIV from the R.KEY_PAIR_PUB or create a forged digital signature due to the use of a weak cryptographic suite by TOE for either key pair generation or digital signature operation. This threat is directly covered by **O.CRYPTO** (Secure Cryptographic Operations).

T.MISUSE is a threat by which a TA.EXTERNAL, TA.INSIDER or a TA.INADVERTENT who is able to access the TOE services uses these services without proper authorisation or in a manner for which they are not intended. This threat is countered by several security objectives. First, several audit trails recorded by the TOE (**O.AUDIT** (Generation and Export of Audit Data)) and later on reviewed by the auditors (**OE.AUDIT_REVIEW** (Audit review)) permit to monitor the security-sensitive activities undertaken during the usage of the TOE services. In particular, the next events (in brackets) are recorded for each TOE service:

- user management (modification of TOE user management data, adding new users or roles, deleting users or roles)
- TSU configuration (changes in the R.CONTEXT, updates of the internal clock values)
- start of TSU operation (TOE initialisation, TOE start-up, start of TSU operation)
- stop of TSU operation (stop of TSU operation)

- key destruction (destruction of R.KEY_PAIR_PUB/ R. KEY_PAIR_PRIV pairs)
- generation of key pair (generation of R.KEY_PAIR_PUB/ R. KEY_PAIR_PRIV pairs)
- public key export for certificate request (export of R.KEY_PAIR_PUB for certificate request)
- certificate import (certificate import)
- timestamp generation and internal audit (updates of the internal clock values, time-stamp generation)

Audit related security objectives intend to mitigate the threat where the threat agent is either a TA.INSIDER or a TA.INADVERTENT. For threat agents TA.EXTERNAL, this threat is countered by authentication and access control mechanisms implemented by the TOE, and represented by the objectives **O.USER_AUTHENTICATION** (Authentication of TOE Users) and **O.RBAC** (Role-based Access Control to TOE Services) respectively. This threat is also countered by **OE.SECURE_OPER** (Secure Operating Procedures), which focuses on procedures and controls implemented by the TOE environment towards ensuring a secure operation of the TOE services. Finally, this threat is diminished by **OE.PERSONNEL** (Liability and Training), which covers the awareness and training of the personnel that use or access the TOE. This objective diminishes the threat in all cases (TA.EXTERNAL, TA.INSIDER or TA.INADVERTENT) due to the liability issues, and also in the case of a TA.INADVERTENT because of the training undertaken. OE.TSS sets up a time-stamping policy, ensuring that the application, organisational and technical measures are enforced against misuse by TA.EXTERNAL, TA.INSIDER or TA.INADVERTENT. These measures include prevention, protection and detection measures, such as access control or audit trails review.

T.INSECURE_INITIALISATION is a threat by which a TA.EXTERNAL, a TA.INSIDER or a TA.INADVERTENT initialises the TOE with insecure R.TSF_DATA. This threat is countered by several security objectives. First, audit trails related to TOE initialisation are recorded by the TOE (**O.AUDIT** (Generation and Export of Audit Data)) and later on reviewed by the auditors (**OE.AUDIT_REVIEW** (Audit review)). This ensures that any initialisation is recorded and appropriately traced back to the corresponding user and date. This threat is also countered by **OE.SECURE_INIT** (Secure Initialisation Procedures), which establishes procedures and controls in the TOE environment aimed at ensuring the secure set-up and initialisation of the TOE services. Finally, this threat is diminished by **OE.PERSONNEL** (Liability and Training), which covers the awareness and training of the personnel that use or access the TOE. This objective diminishes the threat in all cases (TA.EXTERNAL, TA.INSIDER or TA.INADVERTENT) due to the liability issues, and also in the case of a TA.INADVERTENT because of the training undertaken.

T.AUDIT_ALTERATION is a threat where a TA.EXTERNAL or TA.INSIDER alters the TOE R.AUDIT_DATA. This threat is countered by **O.AUDIT_PROTECTION** (Protection of audit data), which states that the TOE shall implement mechanisms to prevent a T.EXTERNAL and T.INSIDER from modifying R.AUDIT_DATA.

OSP.ALGORITHMS states that the TOE shall use only approved algorithms and algorithm parameters defined as acceptable for the key pair generation (R.KEY_PAIR_PUB and private key referred by R_KEY_PAIR_PRIV) and time-stamps signing. The policy includes the generation of random numbers and the quality of the key pairs generated. The aim is to ensure the confidentiality and integrity of private keys (private key referred by R_KEY_PAIR_PRIV) and the integrity of public keys (R.KEY_PAIR_PUB). With this regard, the policy also states that the TOE shall support cryptographic algorithms and key lengths conformant to the rules defined by the relevant national CC Certification Body. This organisational security policy is addressed by several objectives. **O.CRYPTO** (Secure Cryptographic Operations) provides a direct satisfaction of this OSP. Also, as the private key is generated and managed by the TSU only, the TOE is required to ensure the integrity of the public key when it is under its control and before it is exported for certification, as defined by **O.PUBLIC_KEY_MANAGEMENT** (Secure Management of Public Key). On the other hand, the TOE environment has to ensure the confidentiality and integrity of the private key (**OE.PRIVATE_KEY_MANAGEMENT** (Secure Management of Private Key)). Both to ensure this and for the key pair generation (**OE.KEY_PAIR_GENERATION** (Public Key/Private Key Pair Generation)), the TOE environment has to implement secure cryptographic algorithms and parameters compliant with the requirements established by the national authority.

OSP.SERVICE states that the TOE shall generate timestamps in conformity with the time-stamping policy, and where the time-stamps shall be signed using the private key referenced in the R.CONTEXT. This organisational

security policy is addressed by two security objectives. For the TOE, **O.AUDIT** (Generation and Export of Audit Data) requires the TOE to audit a number of events, including the time-stamp generation. For this event some relevant information from the R.CONTEXT has to be incorporated (identification of the time source, the time-stamping policy and the identifier of the key pair used in the time-stamping generation process), ensuring that if the time-stamping policy is wrongly applied, or a private key different to the one referenced in the R.CONTEXT is used, then it will be detected by reviewing the recorded audit trails. For the TOE environment, **OE.AUDIT_REVIEW** (Audit review) mandates the TOE Auditors to check the audit trails on a regular basis, and notify the corresponding authority in the case that an incident occurred.

OSP.REQUEST_MGMT states that the time-stamping protocol implemented by the TOE shall ensure that the time-stamp is generated in conformity with the data received in the request. The requests, as defined in R.REQUEST, include at least the hash of the document to be processed and the identification of the hash algorithm used to calculate the hash of such document. The security objective **OE.TIMESTAMP_VERIFICATION** (Time-stamp verification) meets this policy by establishing that the requester has to verify the correctness of the time-stamps received from the TOE by verifying the digital signature of the time-stamp and checking if the hash within the received time-stamp is the same as the one included in the corresponding request. Consequently, this allows the requester to check whether the time-stamp has been appropriately generated by the TOE according their request.

OSP.CLOCK states that during the initialisation of the TSU, the reference time of the R.DATE_AND_TIME shall be checked to be synchronised with a trusted external UTC time source. This policy is met by **OE.SECURE_INIT** (Secure Initialisation Procedures) by establishing that this check has to be made by the security officer, who has the duty to administer the TSU.

A.TSS assumes that the Time Stamping System meets the requirements laid down in [EN319421] or equivalent. This assumption is directly covered by **OE.TSS** (Time Stamping System).

A.ACCESS_PROTECTED assumes that the TOE is protected by physical and organisational protection measures implemented by the TOE environment, including restricted physical access to the TOE by authorised persons only and shall require dual control. This assumption is covered by **OE.PROTECT_ACCESS** (Prevention of Unauthorised Physical Access), which establishes that the TOE has to be protected by physical, logical and organisational protection measures implemented by the TOE environment in order to prevent any TOE modification, as well as any protected assets disclosure. This objective includes measures to restrict the TOE usage to authorised persons only and that require dual control.

A.REF_TIME indicates that no attack can simultaneously compromise the reference time and the TOE clock checking mechanism, e.g., by changing the synchronization state. This is satisfied by **OE.SECURE_INIT** (Secure Initialisation Procedures), which requires that the synchronisation of the reference time (R.DATE_AND_TIME) with a trusted external UTC time source has to be checked by the security officer during initialisation. Moreover, OE.SECURE_INIT establishes that an attack that compromises simultaneously and in a coherent way the value of the reference time and the synchronisation state has to be counteracted by measures implemented by the TOE environment. Therefore, once the synchronisation is checked during the secure initialisation, the reference time will be necessarily correct or the TOE environment will detect it and stop operation, as any modification afterwards by an attacker can only happen either on the synchronisation state or the reference time, but not both simultaneously.

A.TIMESTAMP_VERIFICATION assumes that the requester verifies the correctness of the time-stamps received from the TOE and ensures its preservation, if needed. This assumption is directly covered by **OE.TIMESTAMP_VERIFICATION** (Time-stamp verification).

A.AUDIT_REVIEW assumes that the TOE Auditors check the audit trails on a regular basis, and notify the corresponding authority in the case that an incident occurred. This assumption is directly covered by **OE.AUDIT_REVIEW** (Audit review).

A.CA assumes that the Certification Authority that issues the certificates to the TOE implements a set of practices in conformity with their CP/CPS. This assumption is directly covered by **OE.CA** (Certification Authority).

A.CERTIFIED_CM assumes that the cryptographic module used by the TOE to digitally sign the time-stamps is a certified device as required in EN 319 421 or equivalent. This assumption is directly covered by **OE.CERTIFIED_CM** (Certified cryptographic module).

A.SECURE_BACKUP assumes that, in the case the cryptographic module used by the TOE supports backup of TSU private keys, they are copied, stored and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment (see A.ACCESS_PROTECTED). The personnel authorised to carry out this function shall be limited to those requiring to do so under the established practices. The assumption also indicates that any backup copies of the TSU private signing keys have to be protected by the cryptographic module to ensure its integrity and confidentiality before being stored outside that device. This assumption is directly covered by **OE.SECURE_BACKUP** (Secure backup of private keys).

8 Security functional requirements

This section describes the operations and security functional requirements that a TOE shall fulfil in order to be compliant to this PP

8.1 Subjects, objects, operations and security attributes

8.1.1 Subjects

We define the following subjects:

- S.OFFICER: Security officer.
- S.REQUESTER: Entity that uses the time-stamp generation service.
- S.AUDITOR: Auditor.

8.1.2 Objects

We define the following list of objects:

- OB.CONTEXT: This object corresponds to the R.CONTEXT.
- OB.TIMESTAMP_TOKEN: This object corresponds to the R.TIMESTAMP_TOKEN.
- OB.TIMESTAMP_REQUEST: This object corresponds to the R.REQUEST.
- OB.PUB_KEY: This object corresponds to the R.KEY_PAIR_PUB.
- OB.PRIV_KEY: This object corresponds to the R.KEY_PAIR_PRIV.
- OB. DATE_AND_TIME: This object corresponds to the R.DATE_AND_TIME.

8.1.3 Operations

We define the following operations:

- OP.CONTEXT_CREATION: creation of OB.CONTEXT, including the request to create a key pair in the HSM.
- OP.CONTEXT_DESTRUCTION: destruction of OB.CONTEXT.
- OP.CONTEXT_MODIFICATION: modification of OB.CONTEXT.
- OP.CONTEXT_CONSULTATION: consultation of OB.CONTEXT.
- OP.PUBLIC_KEY_EXPORT: export of OB.PUB_KEY to obtain the timestamping unit certificate.
- OP.TIMESTAMPING_UNIT_CERTIFICATE_IMPORT: import of the timestamping unit certificate into OB.CONTEXT.
- OP.TIMESTAMP_TOKEN_REQUEST_IMPORT: reception of OB.TIMESTAMP_REQUEST.
- OP.TIMESTAMP_TOKEN_CREATION: generation of OB.TIMESTAMP_TOKEN.
- OP.TIMESTAMP_TOKEN_RESPONSE: sending of OB.TIMESTAMP_TOKEN to S.REQUESTER.

- OP.INIT_DATE_AND_TIME: initialization of OB.DATE_AND_TIME.

8.1.4 Security attributes

For each object, we define a list of security attributes:

8.1.4.1 OB.CONTEXT

- AT.CONTEXT_OPERATIONAL: This attribute indicates if the context is operational or not.
- AT.OPERATIONAL_CONTEXT_COMPLETE: This attribute indicates that all the information needed to create the operational context has been filled in.
- AT.NON_OPERATIONAL_CONTEXT_KEY_PAIR_CREATED: This attribute indicates that the key pair associated with the context has been created.
- AT.MONOTONIC_TIMESTAMP_TOKEN_TIME: This attribute indicates true if the time included in the last issued time-stamp token is greater than the one in the preceding one.
- AT.PRIVATE_KEY_EFFECTIVE_VALIDITY_PERIOD: This attribute indicates the expiration date of the certificate associated with the private key.
- AT.DEFAULT_TIMESTAMPING_POLICY: This attribute describes the default time-stamp policy associated with the context.
- AT.IMPORTED_CERTIFICATE: Value of the timestamping certificate imported into the TOE.
- AT.IMPORTED_CERTIFICATE_PUBLIC_KEY: value of the public key of the non operational context into which the certificate is imported.
- AT.NON_OPERATIONAL_CONTEXT_PRIVATE_KEY: value of reference to the private key of the non operational context into which the certificate is imported.
- AT.IMPORTED_CERTIFICATE_PRIVATE_KEY_VALIDITY_PERIOD: value of the private key validity period contained in the certificate imported into the TOE, if present.
- AT.PUBLIC_KEY_ALGORITHM_IDENTIFIER: value of the public key algorithm identifier.

8.1.4.2 OB.TIMESTAMP_TOKEN

- AT.TIMESTAMP_TOKEN_TIME: value of the time contained in the exported timestamp token
- AT.TIMESTAMPING_UNIT_CERTIFICATE_REFERENCE: value of the certificate reference
- AT.USED_TIMESTAMPING_POLICY_IDENTIFIER: value of the timestamping policy identifier contained in the exported timestamp token
- AT.TIMESTAMP_TOKEN_SIGNATURE: value of the digital signature of the timestamp token.

8.1.4.3 OB.TIMESTAMP_REQUEST

- AT.TIMESTAMP_TOKEN_REQUEST: Value of the imported timestamp token request.
- AT.HASH_ALGORITHM_IDENTIFIER: Value of the hash algorithm identifier used to generate the data imprint contained in the imported timestamp token request.
- AT.DATA_IMPRINT: value of the data imprint contained in the imported timestamp token request

- AT.REQUEST_POLICY_IDENTIFIER: value of the timestamping policy identifier contained in the imported timestamp token request, if present

- AT.REQUEST_NONCE: value of the nonce contained in the imported timestamp token request, if present

8.1.4.4 OB.PUB_KEY

- AT.PUBLIC_KEY_VALUE: value of the public key.

8.1.4.5 OB.PRIV_KEY

- AT.PRIVATE_KEY_VALUE: value of reference to the private key.

8.1.4.6 OB. DATE_AND_TIME

- AT. DATE_AND_TIME_VALUE: This attribute indicates the clock value used by the context.

- AT. DATE_AND_TIME_SYNCHRONIZED: This attribute indicates that the date and time value used by the context is synchronized with UTC.

8.2 Security requirements operations

Common Criteria allows several operations to be performed on functional requirements; refinement, selection, assignment, and iteration are defined in Part 1 of CC. Each of these operations is used in this PP as follows:

- A refinement operation is used to add detail to a requirement, and thus further restricts a requirement. A refinement of a security requirement is included in text as *italicized and underlined* text. In cases where words from a CC requirement were deleted, the deleted text appears ~~crossed out~~.

- A selection operation is used to select one or more options provided by the CC in stating a requirement. A selection is indicated in square brackets with selected option as underlined text, italicized and in blue colour [selection: *minimum*]. Selections left to be filled in by the ST author appear in square brackets with an indication that a selection is to be made, and with the available options italicized and in blue colour [selection*: minimum, basic, detailed, not specified*].

- An assignment operation is used to assign a specific value to an unspecified parameter. An assignment is indicated in square brackets with the specific value as underlined text, italicized and in blue colour [assignment: *none*]. Assignments left to be filled in by the ST author appear in square brackets with an indication that an assignment is to be made, and with the original text italicized and in blue colour [assignment: *other audit relevant information*].

- An iteration operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash “/", and the iteration indicator after the component identifier.

8.3 User Data Protection (FDP)

FDP_ACC.1/Context_Management_Policy Subset access control

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [assignment: *context management policy*] on [assignment:

- *Subjects: subject representing the Security Officer (S.OFFICER) and the auditor (S.AUDITOR),*
- *Objects: timestamping contexts(OB.CONTEXT),*

- *Operations: creation, modification, destruction and consultation of the timestamping contexts (OP.CONTEXT_CREATION, OP.CONTEXT_MODIFICATION, OP.CONTEXT_DESTRUCTION, and OP.CONTEXT_CONSULTATION respectively).*].

FDP_ACF.1/Context_Management_Policy Security attribute based access control

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the [assignment: *context management policy*] to objects based on the following: [assignment:

- *Objects: OB.CONTEXT*
- *SFP-relevant security attributes: AT.CONTEXT_OPERATIONAL, AT.OPERATIONAL_CONTEXT_COMPLETE and AT.NON_OPERATIONAL_CONTEXT_KEY_PAIR_CREATED].*

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment:

- *The creation of a non operational context (OP.CONTEXT_CREATION) is authorized to be performed only by an authenticated Security Officer (S.OFFICER) only if the following required information have been defined for this context (i.e., the value of the security attribute AT.OPERATIONAL_CONTEXT_COMPLETE is "True"):*
    - *the accuracy with UTC time that is guaranteed for the time contained in timestamping tokens.*
    - *reference(s) of accepted timestamping policies.*
    - *identifier(s) of authorized hash algorithms or each timestamping Policy (recommendations for the choice of hash algorithms are provided by national authority).*
- *The consultation of the following information only that are contained in both non operational and operational contexts (OP.CONTEXT_CONSULTATION) is authorized to be performed only by an authenticated Security Officer (S.OFFICER) or an authenticated Auditor (S.AUDITOR):*
    - *the accuracy with UTC time that is guaranteed for the time contained in timestamping tokens.*
    - *reference(s) of accepted timestamping policies.*
    - *identifier(s) of authorized hash algorithms or each timestamping Policy (recommendations for the choice of hash algorithms are provided by national authority).*
    - *the timestamping unit certificate (for operational contexts only).*
- *The modification of all information contained in a non operational context except the key pair value (OP.CONTEXT_MODIFICATION) is authorized to be performed only by an authenticated Security Officer (S.OFFICER) only provided that if the non operational context has not yet been created yet (i.e., the value of the security attribute AT.NON_OPERATIONAL_CONTEXT_KEY_PAIR_CREATED associated with the non operation context is "False").*
- *The destruction of both non operational and operational contexts (OP.CONTEXT_DESTRUCTION) is authorized to be performed by an authenticated Security Officer (S.OFFICER)].*

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *none*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment:

- *the modification of key pairs contained in non operational contexts (i.e., timestamping contexts for which the value of the associated security attribute AT.CONTEXT_OPERATIONAL is "False") is not authorized*
- *the modification of information contained in operational contexts (i.e., timestamping contexts for which the value of the associated security attribute AT.CONTEXT_OPERATIONAL is "True") is not authorized*
- *the Auditor (S.AUDITOR) cannot perform the following operations:*
    - *creation of OB.CONTEXT (OP.CONTEXT_CREATION)*
    - *destruction of OB.CONTEXT (OP.CONTEXT_DESTRUCTION)*
    - *modification of OB.CONTEXT (OP.CONTEXT_MODIFICATION)*].

FDP_ITC.1/Context_Management_Policy Import of user data without security attributes

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_MSA.3 Static attribute initialisation

FDP_ITC.1.1 The TSF shall enforce the [assignment: *context management policy*] when importing user data, controlled under the SFP, from outside of the TOE.

Application Note: The imported user data correspond to the following information involved during the operations of creation and modification of timestamping contexts:

- identification of the time source that shall be used to obtain the time value contained in timestamp tokens,
- accuracy with UTC time that is guaranteed for the time contained in timestamping tokens,
- reference(s) of accepted timestamping policies,
- identifier(s) of authorized hash algorithms for each timestamping policy.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment: *additional importation control rules*].

FDP_SDI.2/Context_Management_Policy Stored data integrity monitoring and action

Dependencies: No dependencies.

FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF for [assignment: *integrity errors*] on all objects, based on the following attributes: [assignment: *user data attributes*]

Application Note: User data correspond to the timestamping contexts.

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall [assignment: *action to be taken*].

FDP_ETC.1/Non_Operational_Context_Public_KeyExport of user data without security attributes

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FDP_ETC.1.1 The TSF shall enforce the [assignment: *key management policy*] when exporting user data, controlled under the SFP(s), outside of the TOE.

Application Note: The exported user data are the public keys of non operational contexts which are generated by the TOE during the context creation phase along with the corresponding public key algorithm identifiers.

FDP_ETC.1.2 The TSF shall export the user data without the user data´s associated security attributes.

FDP_ITC.2/Timestamping_Unit_Certificate Import of user data with security attributes

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

[FTP_ITC.1 Inter-TSF trusted channel, or

FTP_TRP.1 Trusted path]

FPT_TDC.1 Inter-TSF basic TSF data consistency

FDP_ITC.2.1 The TSF shall enforce the [assignment: *key management policy*] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2 The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4 The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment: *rules defined in the key management policy*].

FDP_IFC.1/Key_Management_Policy Subset information flow control

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [assignment: *key management policy*] on [assignment:

- *Information:*
  - *value of the timestamping unit certificate imported into the TOE (AT.IMPORTED_CERTIFICATE),*
  - *value of the public key contained in the timestamping unit certificate imported into the TOE (AT.IMPORTED_CERTIFICATE_PUBLIC_KEY),*
  - *value of the public key of the non operational context into which the certificate is imported (AT.PUBLIC_KEY_VALUE),*
  - *value of reference to the private key of the non operational context into which the certificate is imported (AT.PRIVATE_KEY_VALUE),*
  - *value of the public key algorithm identifier (AT.PUBLIC_KEY_ALGORITHM_IDENTIFIER).*
- *Subjects:*
  - *Security Officer (S.OFFICER).*
- *Operations:*
  - *export of the public key to obtain the timestamping unit certificate (OP.PUBLIC_KEY_EXPORT),*
  - *import of the timestamping unit certificate (OP.TIMESTAMPING_UNIT_CERTIFICATE_IMPORT).*
- *Objects:*
  - *timestamping contexts (OB.CONTEXT),*
  - *key pair (OB.PUB_KEY and OB.PRIV_KEY)*].

FDP_IFF.1/Key_Management_Policy Simple security attributes

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1 The TSF shall enforce the [assignment: *key management policy*] based on the following types of subject and information security attributes: [assignment:

- *the security attributes AT.OPERATIONAL_CONTEXT_COMPLETE and AT.NON_OPERATIONAL_CONTEXT_KEY_PAIR_CREATED associated with a non operational context (OB.CONTEXT with security attribute AT.CONTEXT_OPERATIONAL being "False") that indicate respectively if the non operational context is complete (i.e., all required information are specified) and if the non operational context has been created by the Security Officer,*
- *the security attribute AT.CONTEXT_OPERATIONAL that indicates that a timestamping context (OB.CONTEXT) is operational following the authorized import of the timestamping unit certificate.*].

Application Note: The ST author can specify other security attributes on which other rules of the key management policy would be based.

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment:

- *the operation OP.PUBLIC_KEY_EXPORT enables the export of the public key of a non operational context and the identifier of the public key algorithm (AT.PUBLIC_KEY_VALUE and AT.PUBLIC_KEY_ALGORITHM_IDENTIFIER) from the non operational context (OB.CONTEXT with security attributes AT.CONTEXT_OPERATIONAL being "False" and AT.NON_OPERATIONAL_CONTEXT_KEY_PAIR_CREATED being "True") by the subject that exports the public key (S.OFFICER). This operation is authorized to be performed only on behalf of an authenticated Security Officer,*
- *the operation OP.TIMESTAMPING_UNIT_CERTIFICATE_IMPORT enables the import of the certificate corresponding to the exported public key (AT.IMPORTED_CERTIFICATE) into the non operational context (OB.CONTEXT with security attribute AT.CONTEXT_OPERATIONAL being "False") by the subject that imports the certificate (S.OFFICER) in order to create the corresponding operational context (OB.CONTEXT with security attribute AT.CONTEXT_OPERATIONAL being "True"). This operation is authorized to be performed only on behalf of an authenticated Security Officer only if the following conditions hold:*
- *the non operational context is both complete and created (the value of the security attributes AT.OPERATIONAL_CONTEXT_COMPLETE and AT.NON_OPERATIONAL_CONTEXT_KEY_PAIR_CREATED are both "True"),*
- *the value of the public key of the imported certificate (AT.IMPORTED_CERTIFICATE_PUBLIC_KEY) corresponds to the value of the public key of the non operational context into which the timestamping certificate is imported (AT.PUBLIC_KEY_VALUE)*].

FDP_IFF.1.3 The TSF shall enforce the [assignment: *additional information flow control SFP rules*].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [assignment: *destruction of the private key of an operational context if the associated effective private key validity period (AT.PRIVATE_KEY_EFFECTIVE_VALIDITY_PERIOD) has expired*].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [assignment: *timestamping certificates (AT.IMPORTED_CERTIFICATE) shall not be imported into an operational context (OB.CONTEXT with security attribute AT.CONTEXT_OPERATIONAL being "True")*]

FDP_ITC.1/Date_and_Time Import of user data without security attributes

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_MSA.3 Static attribute initialisation

FDP_ITC.1.1 The TSF shall enforce the [assignment: *timestamp token generation policy*] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment: *additional importation control rules*].

FDP_ACC.1/Timestamp_Token_Generation_PolicySubset access control

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [assignment: *timestamp token generation policy*] on [assignment:

- *Subjects: none*
- *Objects:*
  - *operational contexts (OB.CONTEXT with security attribute AT.CONTEXT_OPERATIONAL being "True") generating timestamp tokens signed against the context signature private key, the value of the timestamping unit certificate reference (AT.IMPORTED_CERTIFICATE_PUBLIC_KEY) and the value of the used timestamping policy (AT.DEFAULT_TIMESTAMPING_POLICY),*
  - *generated timestamp tokens (OB.TIMESTAMP_TOKEN) containing the information present in the corresponding timestamp token requests (OB.TIMESTAMP_REQUEST),*
  - *the internal clock (OB. DATE_AND_TIME) with the time value provided by the used internal clock (AT. DATE_AND_TIME_VALUE),*
- *Operations: creation and sending of timestamp tokens (OP.TIMESTAMP_TOKEN_CREATION and OP.TIMESTAMP_TOKEN_RESPONSE)*].

FDP_ACF.1/Timestamp_Token_Generation_Policy Security attribute based access control

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the [assignment: *timestamp token generation policy*] to objects based on the following: [assignment:

- *Objects: OB.CONTEXT*
- *SFP-relevant security attributes:*
  - *the security attribute AT.CONTEXT_OPERATIONAL that indicates if the timestamping context (OB.CONTEXT) whose information are used to generate the timestamp token is operational,*
  - *the security attribute AT.PRIVATE_KEY_EFFECTIVE_VALIDITY_PERIOD associated with the used operational context (OB.CONTEXT with security attribute AT.CONTEXT_OPERATIONAL being "True") that indicates the validity period of the context private key,*
  - *the security attribute AT.MONOTONIC_TIMESTAMP_TOKEN_TIME associated with the used operational context (OB.TIMESTAMPING_CONTEXT) that indicates if the time value provided by the used internal clock for the current timestamp token is greater than the time value placed in the previous timestamp token generated by this timestamping context,*
  - *the security attribute AT.DATE_AND_TIME_SYNCHRONIZED associated with the used operational context (OB.CONTEXT with security attribute AT.CONTEXT_OPERATIONAL being "True") that indicates if the internal clock is synchronized with UTC with the accuracy specified in the operational context,*
  - *the global security attribute AT.DEFAULT_TIMESTAMPING_POLICY_DEFINED that indicates if a default timestamping policy has been defined for the timestamping system using a policy identifier by an authenticated Security Officer].*

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment:

- *the creation of timestamp tokens (OP.TIMESTAMP_TOKEN_CREATION on OB.TIMESTAMP_TOKEN) is authorized to be performed only in an automatic way by the TOE if the following conditions hold:*
    - *the context whose information are used to generate the timestamp token is operational (the security attribute AT.CONTEXT_OPERATIONAL associated with OB.CONTEXT is "True"),*
    - *the time value provided by the internal clock of the used timestamping context is greater than the time value placed in the previous timestamp token generated by this context (the security attribute AT.MONOTONIC_TIMESTAMP_TOKEN_TIME is "True"),*
    - *the context whose information are used to generate the timestamp token supports the timestamping policy specified in the token request or the default timestamping policy when no timestamping policy has been specified in the token request (the global security attribute AT.DEFAULT_TIMESTAMPING_POLICY is defined),*
    - *the used internal clock is synchronized with UTC with the accuracy defined in the used operational context (the security attribute AT.DATE_AND_TIME_SYNCHRONIZED is "True"),*
- *the signature of timestamp tokens (OP.TIMESTAMP_TOKEN_SIGNATURE on OB.TIMESTAMP_TOKEN) is authorized to be performed only in an automatic way by the TOE if the following conditions hold:*
    - *the context whose information are used to generate the timestamp token is operational (the security attribute AT.CONTEXT_OPERATIONAL associated with OB.CONTEXT is "True"),*
    - *the context private key used to generate the signature of the timestamp token is valid (the date and time of the signature generation is included in the private key validity period defined by the security attribute AT.PRIVATE_KEY_EFFECTIVE_VALIDITY_PERIOD associated with the operational context),*
    - *the internal clock is synchronized with UTC with the accuracy defined in the used operational context (the security attribute AT.DATE_AND_TIME_SYNCHRONIZED is "True")].*

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *none*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: *none*]

8.4 Security Management (FMT)

FMT_MSA.1/Context_Management_Policy Management of security attributes

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [assignment: *context management policy*] to restrict the ability to [selection: *query and modify*] the security attributes [assignment: *AT.OPERATIONAL_CONTEXT_COMPLETE, AT.NON_OPERATIONAL_CONTEXT_KEY_PAIR_CREATED and AT.CONTEXT_OPERATIONAL*] to [assignment: *Security Officer (S.OFFICER)*].

Application Note: The modification operation on the security attributes AT.OPERATIONAL_CONTEXT_COMPLETE and AT.CONTEXT_OPERATIONAL is performed indirectly by the Security Officer (S.OFFICER), since these attribute modifications result from operations performed by the S.OFFICER (OP.CONTEXT_CREATION and OP.TIMESTAMPING_UNIT_CERTIFICATE_IMPORT). The S.OFFICER can only specify that a non operational context is created (i.e., the S.OFFICER can only modify the security attribute AT.NON_OPERATIONAL_CONTEXT_KEY_PAIR_CREATED from the "False" to the "True" value only). The security attribute AT.NON_OPERATIONAL_CONTEXT_KEY_PAIR_CREATED indicates that all required information of a non operational context have been specified and that the corresponding context has been created (i.e., validated) by the S.OFFICER.

FMT_MSA.1/Multiple_Policies Management of security attributes

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [assignment: *context management policy, key management policy, timestamp token generation policy*] to restrict the ability to [selection: *query and modify*] the security attributes [assignment: *AT.MONOTONIC_TIMESTAMP_TOKEN_TIME*] to [assignment: *none*].

Application Note: The value of the security attribute AT.MONOTONIC_TIMESTAMP_TOKEN_TIME is set to the "True" value by the TOE to enable the first timestamp token to be generated by an operational context.

FMT_MSA.3/Context_Management_Policy Static attribute initialisation

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [assignment: *context management policy*] to provide [selection: *restrictive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [assignment: *none*] to specify alternative initial values to override the default values when an object or information is created.

FMT_SMF.1/Context_Management_Policy Specification of Management Functions

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [assignment:

- *modification and query of the following security attributes:*
  - *AT.OPERATIONAL_CONTEXT_COMPLETE*
  - *AT.NON_OPERATIONAL_CONTEXT_KEY_PAIR_CREATED*
  - *AT.CONTEXT_OPERATIONAL*
  - *AT.MONOTONIC_TIMESTAMP_TOKEN_TIME*].

FMT_MSA.1/Date_and_Time Management of security attributes

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [assignment: *timestamp token generation policy*] to restrict the ability to [selection: *query and modify*] the security attributes [assignment: *AT.DATE_AND_TIME_SYNCHRONIZED*] to [assignment: *Security Officer (S.OFFICER)*].

FMT_MSA.3/Date_and_Time Static attribute initialisation

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [assignment: *timestamp token generation policy*] to provide [selection: *restrictive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [assignment: *Security Officer (S.OFFICER)*] to specify alternative initial values to override the default values when an object or information is created.

FMT_SMF.1/Date_and_Time Specification of Management Functions

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [assignment:

- *query the security attribute AT. DATE_AND_TIME_SYNCHRONIZED,*
- *set the security attribute AT. DATE_AND_TIME_SYNCHRONIZED to "Synchronized" if the internal clock is synchronized with UTC with the accuracy defined in the used operational context,*
- *set the security attribute AT. DATE_AND_TIME_SYNCHRONIZED to "Not synchronized" if the internal clock is not synchronized with UTC with the accuracy defined in the used operational context,*
- *synchronize the internal clock of a timestamping unit,*
- *periodically compare the time difference between the internal clock of a timestamping unit with UTC: if the time difference is greater than the authorized value AT. DATE_AND_TIME_SYNCHRONIZED is set to "Not synchronized",*
- *periodically record the time difference between the internal clock of a timestamping unit with UTC to create and update a log of those time differences,*
- *periodically verify the synchronization of the internal clock of a timestamping unit by making use of the history of time differences between this internal clock and UTC: if the history of the time differences is not in conformance with the drift authorized over a given time period then AT. DATE_AND_TIME_SYNCHRONIZED is set to "Not synchronized",*
- *initialize the internal clock during the initialization phase of a timestamping unit by synchonizing it with UTC.*]

Application Note: Period of comparison, authorized value, and length of the time difference history shall be set to meet the requirements of [EN319421] or equivalent.

FMT_MTD.1/Date_and_Time Management of TSF data

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to [selection: [assignment: *initialize (OP.INIT_DATE_AND_TIME)*]] the [assignment: *internal clock of a timestamping unit (OB. DATE_AND_TIME)*] to [assignment: *Security Officer (S.OFFICER)*].

FMT_SMF.1/Temporary_Interruption Specification of Management Functions

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [assignment:

- *supervision of the synchronization of the TOE,*
- *interruption of the timestamping service in the following cases: the state of the internal clock is "Not synchronized" for the operational context used to generate timestamp tokens (i.e., the security attribute AT. DATE_AND_TIME_SYNCHRONIZED is "False"),*]

FMT_SMR.1 Security roles

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [assignment: *Security Officer (S.OFFICER) and Auditor (S.AUDITOR)*].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

8.5 Protection of the TSF (FPT)

FPT_TDC.1/Timestamping_Unit_Certificate Inter-TSF basic TSF data consistency

Dependencies: No dependencies.

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [assignment: *fields of the imported timestamping unit certificates*] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use [assignment: *the value of the public key contained in the imported certificate to verify it corresponds to the value of the non operational context public key generated during the context creation phase*] when interpreting the TSF data from another trusted IT product

FPT_STM.1 Reliable time stamps

Dependencies: No dependencies.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

8.6 Trusted Path/Channels (FTP)

FTP_TRP.1/Timestamping_Unit_Certificate Trusted path

Dependencies: No dependencies.

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [selection: *local*] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [selection: *modification, disclosure*].

FTP_TRP.1.2 The TSF shall permit [selection: *local users*] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [selection: *initial user authentication*]

Application note: Local users referred to in these requirements are the Security Officers (S.OFFICER) of the TOE who import timestamping unit certificates into the TOE.

8.7 Cryptographic Support (FCS)

FCS_CKM.1 Cryptographic key generation

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or

FCS_COP.1 Cryptographic operation]

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic key generation algorithm*] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*]. *The standards shall be selected from the list of approved algorithms and parameters, in accordance with national guidance, and subject to each Certification Body. Notwithstanding, recommendations for algorithms and parameters for secure electronic signatures are given in [ETSI 119 312] and [SOG-IS-Crypto].*

Application note: This requirement concerns the asymmetric key pairs used to create and verify the signature of timestamping tokens generated by a timestamping unit. The key pair shall be generated by the cryptographic module, whereas the key pair generation shall be invoked by the TOE.

FCS_CKM.4 Cryptographic key destruction

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].

Application note: This requirement concerns private keys contained in both operational and non operational contexts. This operation is performed by the cryptographic module on demand of the TOE.

FCS_COP.1 Cryptographic operation

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [assignment: *digital signing*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*]. *The standards shall be selected from the list of approved algorithms and parameters, in accordance with national guidance, and subject to each Certification Body. Notwithstanding, recommendations for algorithms and parameters for secure electronic signatures are given in [ETSI 119 312] and [SOG-IS-Crypto].*

Application note: This requirement refers to digitally signing the timestamp tokens generated by the TOE.

8.8 Identification and Authentication (FIA)

FIA_UID.2 User identification before any action

Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each ~~user~~ *Security Officer (S.OFFICER) and Auditor (S.Auditor)* to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.2 User authentication before any action

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each ~~user~~ Security *Officer (S.OFFICER) and Auditor (S.Auditor)* to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

8.9 Security Audit (FAU)

FAU_GEN.1 Audit data generation

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [selection: *detailed*] level of audit; and

c) [assignment:

- *TOE initialisation,*
- *TOE start-up,*
- *Start of TSU operation,*

- *Stop of TSU operation,*
- *Generation of OB.KEY_PUB and OB.KEY_PRIV pairs*
- *Export of OB.KEY_PUB for certificate request*
- *Certificate import*
- *Destruction of OB.KEY_PUB and OB.KEY_PRIV pairs*
- *Time-stamp generation*
- *Users and roles management operations*
- *Successful and unsuccessful operations, including*
    - *Attempts of initiating a user session.*
    - *Changes of privileges assigned to any role.*
    - *Access to the security attributes of the TOE.*
    - *Unsuccessful attempts to access the TOE resources.*
- *State changes in OB.CONTEXT*
- *Exporting and deleting of audit trail records*
- *Last successful synchronization check,*
- *Manual synchronization (date of synchronization operation and value of synchronization correction),*].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other audit relevant information*].

FAU_SAR.1 Audit review

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [assignment: *Security Officers (S.OFFICER) and Auditors (S.AUDITOR)*] with the capability to read [assignment: *list of audit information*] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.3 Selectable audit review

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to [assignment: *apply searching, sorting and ordering*] of audit data based on [assignment: *type of events, date of events*].

FAU_STG.2 Guarantees of audit data availability

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.2.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.2.2 The TSF shall be able to [selection: *prevent*] unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.2.3 The TSF shall ensure that [assignment: *metric for saving audit records*] stored audit records will be maintained when the following conditions occur: [selection: *audit storage exhaustion, failure, attack*]

FAU_STG.4 Prevention of audit data loss

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall [selection: choose one of: *"ignore audited events", "prevent audited events, except those taken by the authorised user with special rights", "overwrite the oldest stored audit records"*] and [assignment: *other actions to be taken in case of audit storage failure*] if the audit trail is full.

9 Security assurance requirements

The development and the evaluation of the TOE shall be done in accordance with security assurance requirements corresponding to the Evaluation Assurance Level 4 augmented (EAL4+) with ALC_FLR.3 Systematic flaw remediation.

Assurance Class	Assurance Component
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification

Assurance Class	Assurance Component
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis

Table 1 — Security Assurance Requirements: EAL4+ ALC_FLR.3

10 Security requirements rationale

10.1 Security functional requirements rationale

10.1.1 SFR dependencies rationale

The following table displays the SFR dependencies:

SFR	Required Dependency	Dependency Satisfaction
User Data Protection		
FDP_ACC.1/Context_Management_Policy	• FDP_ACF.1	• FDP_ACF.1/Context_Management_Policy
FDP_ACF.1/Context_Management_Policy	• FDP_ACC.1 • FMT_MSA.3	• FDP_ACC.1/Context_Management_Policy • FMT_MSA.3/Context_Management_Policy
FDP_ITC.1/Context_Management_Policy	• [FDP_ACC.1 or FDP_IFC.1] • FMT_MSA.3	• FDP_ACC.1/Context_Management_Policy • FMT_MSA.3/Context_Management_Policy •
FDP_SDI.2/Context_Management_Policy	None	N/A
FDP_ETC.1/Non_Operational_Context_Public_Key	• [FDP_ACC.1 or FDP_IFC.1]	• FDP_IFC.1/Key_Management_Policy
FDP_ITC.2/Timestamping_Unit_Certificate	• [FDP_ACC.1 OR FDP_IFC.1] • [FTP_ITC.1 OR FTP_TRP.1] • FPT_TDC.1	• FDP_IFC.1/Key_Management_Policy • FTP_TRP.1/Timestamping_Unit_Certificate • FPT_TDC.1/Timestamping_Unit_Certificate
FDP_IFC.1/Key_Management_Policy	• FDP_IFF.1	• FDP_IFF.1/Key_Management_Policy •

FDP_IFF.1/Key_Management_Policy	• FDP_IFC.1 • FMT_MSA.3	• FDP_IFC.1/Key_Management_Policy • FMT_MSA.3/Date_and_Time
FDP_ITC.1/Date_and_Time	• [FDP_ACC.1 or FDP_IFC.1] • FMT_MSA.3	• FDP_ACC.1/Context_Management_Policy • FDP_IFC.1/Key_Management_Policy • FMT_MSA.3/Context_Management_Policy • FMT_MSA.3/Date_and_Time
FDP_ACC.1/Timestamp_Token_Generation_Policy	• FDP_ACF.1	• FDP_ACF.1/Timestamp_Token_Generation_Policy
FDP_ACF.1/Timestamp_Token_Generation_Policy	• FDP_ACC.1 • FMT_MSA.3	• FDP_ACC.1/Timestamp_Token_Generation_Policy • FMT_MSA.3/Timestamp_Token_Generation_Policy
Security Management		
FMT_MSA.1/Context_Management_Policy	• [FDP_ACC.1 or FDP_IFC.1] • FMT_SMR.1 • FMT_SMF.1	• FDP_ACC.1/Context_Management_Policy • FMT_SMR.1 • FMT_SMF.1/Context_Management_Policy
FMT_MSA.1/Multiple_Policies	• [FDP_ACC.1 or FDP_IFC.1] • FMT_SMR.1 • FMT_SMF.1	• FDP_ACC.1/Context_Management_Policy • FDP_IFC.1/Key_Management_Policy • FMT_SMR.1 • FMT_SMF.1/Context_Management_Policy • FMT_SMF.1/Temporary_Interruption • FMT_SMF.1/Date_and_Time
FMT_MSA.3/Context_Management_Policy	• FMT_MSA.1 • FMT_SMR.1	• FMT_MSA.1/Context_Management_Policy • FMT_SMR.1
FMT_SMF.1/Context_Management_Policy	None	N/A
FMT_MSA.1/Date_and_Time	• [FDP_ACC.1 or FDP_IFC.1] • FMT_SMR.1 • FMT_SMF.1	• FDP_ACC.1/Timestamp_Token_Generation_Policy • FMT_SMR.1 • • FMT_SMF.1/Date_and_Time
FMT_MSA.3/Date_and_Time	• FMT_MSA.1 • FMT_SMR.1	• FMT_MSA.1/Date_and_Time • FMT_SMR.1
FMT_SMF.1/ Date_and_Time	None	N/A
FMT_MTD.1/ Date_and_Time	• FMT_SMR.1 • FMT_SMF.1	• FMT_SMR.1 • FMT_SMF.1/Date_and_Time
FMT_SMF.1/Temporary_Interruption	None	N/A

FMT_SMR.1	• FIA_UID.1	• FIA_UID.2
Protection of the TSF		
FPT_TDC.1/Timestamping_Unit_Certificate	None	N/A
FPT_STM.1	None	N/A
Trusted Path/Channels		
FTP_TRP.1/Timestamping_Unit_Certificate	None	N/A
Cryptographic Support		
FCS_CKM.1	• [FCS_CKM.2 or FCS_COP.1] • FCS_CKM.4	• FCS_COP.1 • FCS_CKM.4
FCS_CKM.4	• [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	• FCS_CKM.1
FCS_COP.1	• [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] • FCS_CKM.4	• FCS_CKM.1 • FCS_CKM.4
Identification and Authentication		
FIA_UID.2	None	N/A
FIA_UAU.2	• FIA_UID.1	• FIA_UID.2
Security Audit		
FAU_GEN.1/	• FPT_STM.1	• FPT_STM.1
FAU_SAR.1	• FAU_GEN.1	• FAU_GEN.1
FAU_SAR.3	• FAU_SAR.1	• FAU_SAR.1
FAU_STG.2	• FAU_GEN.1	• FAU_GEN.1
FAU_STG.4	• FAU_STG.1	• FAU_STG.2

10.1.2 SFR vs TOE security objectives rationale

The following table shows the correspondence between the security objectives applicable to the TOE and the defined security functional requirements.

	O.AUDIT	O.USER_AUTHENTICATION	O.RBAC	O.PUBLIC_KEY_MANAGEMENT	O.SYNCHRONISATION	O.AUDIT_PROTECTION	O.CRYPTO
FDP_ACC.1/Context_Management_Policy			X				
FDP_ACF.1/Context_Management_Policy			X				
FMT_MSA.3/Context_Management_Policy			X	X			
FMT_MSA.1/Context_Management_Policy			X	X			
FMT_MSA.1/Multiple_Policies			X	X			
FMT_SMF.1/Context_Management_Policy				X			
FDP_ITC.1/Context_Management_Policy				X			
FDP_SDI.2/Context_Management_Policy				X			
FDP_ETC.1/Non_Operational_Context_Public_Key				X			
FDP_ITC.2/Timestamping_Unit_Certificate				X			
FPT_TDC.1/Timestamping_Unit_Certificate				X			
FTP_TRP.1/Timestamping_Unit_Certificate				X			
FDP_IFC.1/Key_Management_Policy				X			
FDP_IFF.1/Key_Management_Policy				X			
FCS_CKM.1							X
FCS_CKM.4							X
FMT_MSA.3/Date_and_Time					X		
FMT_MSA.1/Date_and_Time					X		
FMT_SMF.1/Date_and_Time					X		
FMT_MTD.1/Date_and_Time					X		

	O.AUDIT	O.USER_AUTHENTICATION	O.RBAC	O.PUBLIC_KEY_MANAGEMENT	O.SYNCHRONISATION	O.AUDIT_PROTECTION	O.CRYPTO
FDP_ITC.1/Date_and_Time					X		
FMT_SMF.1/Temporary_Interruption					X		
FDP_ACC.1/Timestamp_Token_Generation_Policy			X				
FDP_ACF.1/Timestamp_Token_Generation_Policy			X				
FCS_COP.1							X
FMT_SMR.1		X					
FIA_UID.2		X					
FIA_UAU.2		X					
FAU_GEN.1	X						
FAU_SAR.1	X						
FAU_SAR.3	X						
FPT_STM.1	X				X		
FAU_STG.4						X	
FAU_STG.2						X	

Table 2 — Mapping between Security Objectives and Security Functional Requirements

Security functional requirements (SFR) coverage is met as each security objective is addressed by at least one SFR, and every SFR is mapped to at least one security objective.

Next, the rationale for each matching is provided:

O.AUDIT is covered by FAU_GEN.1, which ensures that event audit trails are generated by FPT_STM.1, which ensures that the date and time is reliable. Moreover, this objective is also covered by FAU_SAR.1 and by FAU_SAR.3, ensuring the consultation of the audit logs.

O.USER_AUTHENTICATION is covered by FIA_UID.2 and FIA_UAU.2, requiring identification and authentication of the different users and roles before any administrative or audit operation can take place. Moreover, this objective is also covered by FMT_SMR.1 requiring the maintenance of the different roles by the TOE.

O.RBAC is covered by the context management policy :

- FDP_ACC.1/Context_Management_Policy,
- FDP_ACF.1/Context_Management_Policy,
- FMT_MSA.1/Context_Management_Policy
- FMT_MSA.1/Multiple_Policies
- FMT_MSA.3/Context_Management_Policy

In particular, this policy controls the operation for creating and modifying timestamping context. This Objective is also covered by the Time Stamping token generation policy (FDP_ACC.1/Timestamp_Token_Generation_Policy, FDP_ACF.1/Timestamp_Token_Generation_Policy)

O.PUBLIC_KEY_MANAGEMENT is first covered by the context management policy:

- FMT_MSA.1/Context_Management_Policy
- FMT_MSA.1/Multiple_Policies
- FMT_MSA.3/Context_Management_Policy
- FMT_SMF.1/ Context_Management_Policy and
- FDP_SDI.2/Context_Management_Policy

In particular, this policy controls the operation for creating, modifying, consulting and destroying the timestamping context. It is also covered by FDP_ITC.1/Context_Management_Policy which refers to the time stamping context management policy regarding to the import of information needed for context creation.

This objective is also covered by FDP_ETC.1/Non_Operational_Context_Public_Key and FDP_ITC.2/Timestamping_Unit_Certificate, referring to the key management policy regarding the export of the public key and the import of the corresponding certificate.

FPT_TDC.1/Timestamping_Unit_Certificate ensures an adequate interpretation of particular certificates fields, particularly the value of the public key. Moreover, FTP_TRP.1/Timestamping_Unit_Certificate ensures a trusted path with the Administrator when importing the Timestamping unit certificate.

This objective is also covered by the Key Management (FDP_IFC.1/Key_Management_Policy and FDP_IFF.1/Key_Management_Policy)

O.SYNCHRONISATION is covered by FMT_MTD.1/Date_and_Time, ensuring that the internal date and time is initially synchronized by an administrator during the time stamping initialisation process. It is also ensured by FMT_SMF.1/Date_and_Time, requiring a following of the synchronisation with UTC according to a specific precision level. This objective is also covered by FDP_ITC.1/Date_and_Time, referring to the timestamping generation policy based on the synchronization state. FMT_MSA.1/Date and Time and FMT_MSA.3/Date_and_Time are also covering this objective due to the limitation of modifying the

synchronization state to an authenticated Security Officer. FPT_STM.1 ensures that the date associated to each event is reliable.

This objective is covered FMT_SMF.1/Temporary_Interruption, ensuring the monitoring of the synchronization state of the timestamping service and ensures the stop of the service in case of lose of synchronization.

O.AUDIT_PROTECTION is covered by FAU_STG.2 and FAU_STG.4. These objectives protect the audit logs in integrity and ensure the availability of the logs.

O.CRYPTO is covered by all SFRs related to cryptographic key management and cryptographic operations:

- FCS_COP.1
- FCS_CKM.4
- FCS_CKM.1

10.2 Security assurance requirements rationale

We discuss in this section the rationale concerning the security assurance requirements (SAR). First we provide a SAR table with the dependencies and the SAR components that meet them. Second, we discuss the selection of the EAL given in section 10.2.2.

10.2.1 Assurance level table

Assurance Element	Required Dependency	Element Satisfying the Dependency
ADV_ARC.1	(ADV_FSP .1) and (ADV_TDS.1)	ADV_FSP.4, ADV_TDS.3
ADV_FSP.4	(ADV_TDS.1)	ADV_TDS.3
ADV_TDS.3	(ADV_FSP .4)	ADV_FSP.4
AGD_OPE.1	(ADV_FSP.1)	ADV_FSP.4
AGD_PRE.1	No dependency	
ADV_IMP.1	(ADV_TDS.3) and (ALC_TAT.1)	ADV_TDS.3, ALC_TAT.1
ALC_CMC.3	(ALC_CMS.1) and (ALC_DVS.1) and (ALC_LCD.1)	ALC_CMS.3, ALC_DVS.1, ALC_LCD.1
ALC_CMS.3	No dependency	
ALC_DEL.1	No dependency	
ALC_DVS.1	No dependency	
ALC_FLR.3	No dependency	
ALC_LCD.1	No dependency	
ALC_TAT.1	ADV_IMP.1	ADV_IMP.1

ASE_CCL.1	(ASE_ECD.1) and (ASE_INT.1) and (ASE_REQ.1)	ASE_ECD.1, ASE_INT.1, ASE_REQ.2
ASE_ECD.1	No dependency	
ASE_INT.1	No dependency	
ASE_OBJ.2	(ASE_SPD.1)	ASE_SPD.1
ASE_REQ.2	(ASE_ECD.1) and (ASE_OBJ.2)	ASE_ECD.1, ASE_OBJ.2
ASE_SPD.1	No dependency	
ASE_TSS.1	(ADV_FSP.1) and (ASE_INT.1) and (ASE_REQ.1)	ADV_FSP.4, ASE_INT.1, ASE_REQ.2
ATE_COV.2	(ADV_FSP.2) and (ATE_FUN.1)	ADV_FSP.4, ATE_FUN.1
ATE_DPT.1	(ADV_ARC.1) and (ADV_TDS.2) and (ATE_FUN.1)	ADV_ARC.1, ADV_TDS.3, ATE_FUN.1
ATE_FUN.1	(ATE_COV.1)	ATE_COV.2
ATE_IND.2	(ADV_FSP.2) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_COV.1) and (ATE_FUN.1)	ADV_FSP.4, AGD_OPE.1, AGD_PRE.1, ATE_COV.2, ATE_FUN.1
AVA_VAN.3	(ADV_ARC.1) and (ADV_FSP.2) and (ADV_IMP.1) and (ADV_TDS.3) and (AGD_OPE.1) and (AGD_PRE.1)	ADV_ARC.1, ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, AGD_OPE.1, AGD_PRE.1

10.2.2 EAL rationale

The Security Assurance Requirements (SAR) for this Protection Profile have been selected according to the Evaluation Assurance Level 4 augmented (EAL4+) ALC_FLR.3.

EAL4 allows a developer to attain a reasonably high assurance level without the need for highly specialized processes and practices. It is considered to be the highest level that could be applied to an existing product line without undue expense and complexity. As such, EAL4+ ALC_FLR.3 is appropriate for commercial products that can be applied to moderate to medium-high security functions, and resist to enhanced-basic attack potential. The TOE described in this Protection Profile is such a product.