Direction centrale de la sécurité des systèmes d'information

Time-stamping System Protection Profile

Date	**:**	July 18, 2008
Reference	**:**	PP-SH-CCv3.1
Version	**:**	1.7

Courtesy Translation

Courtesy translation of the protection profile registered and certified by the French Certification Body under the reference DCSSI-PP-2008/07.

Table of Contents

Table of Figures

Table of Tables

1 PP introduction

1.1 PP reference

Title:	Time-stamping system Protection Profile
Author:	Trusted Labs
Version:	1.7
Date:	July 18, 2008
Sponsor:	DCSSI
CC version:	3.1 Revision 2

This protection profile is compliant with Common Criteria part 2 and 3 ([CC2] and [CC3]).

The evaluation assurance level required by this protection profile is EAL3+ (EAL3 augmented with AVA_VAN.3 and ALC_FLR.3) specified by the DCSSI *qualification* process [QUA-STD].

1.2 Protection Profile presentation

This protection profile specifies the security requirements for a time-stamping system which consists of at least a time-stamping unit and of administration and supervision components used to provide time-stamping services. The time-stamping system delivers time-stamp tokens. A time-stamp token provides an association between the digest of a document (generated by the application of a hash function on the document to be time-stamped) and a time mark. Time-stamping systems provide elements of evidence contributing to the proof of existence of a document, of possession, or of engagement of a signer.

Thereafter, a **time-stamping unit** is defined as a set of hardware (including an internal clock) and software creating time-stamp tokens and identifiable by a name defined by the time-stamping authority (TSA) and a Certification Authority (CA). Consequently, a time-stamping unit does not exist as such before the certificate issued by the Certification Authority and allowing this identification is present in the system.

In order to introduce all the information required in the time-stamping unit definition, concepts of operational and non operational time-stamping contexts are introduced. A **non operational time-stamping context** is the set of following information:

- the identification of the internal clock that shall be used to obtain the time value contained in time-stamp tokens,
- the guaranteed accuracy with UTC time for the time contained in time-stamp tokens,
- the key pair value (and the identifier of the public-key algorithm) for the creation and the verification of the time-stamp tokens signature,
- the private key validity period defined during the non operational context creation phase,

- the reference(s) of supported time-stamp policies,
- the identifier(s) of hash algorithms for each time-stamp policy.

An **operational time-stamping context** is composed of information of a non operational time-stamping context with the following additional information:

- the effective validity period of the private key associated with the operational context defined at the time of the certificate importation (by taking into account the extension, if present in the certificate, indicating the validity period of the private key),
- the certificate of the time-stamping unit issued by a Certification Authority.

A time-stamping unit uses information of an operational context and the value of the internal clock synchronized with UTC. The internal clock synchronization relies on:

- the initial internal clock synchronization during the time-stamping unit initialization with a time source whose accuracy is known compared to a source UTC (k),
- the monitoring of the internal clock drift and the maintenance of synchronization with the time reference during the normal operation of the time-stamping unit.

The time reference is a local approximation of the UTC time which is obtained from one or several time sources whose accuracy is known compared to one or more UTC (k) sources. The manner of establishing this time reference is not required in this protection profile but it must be specified in the security targets claiming conformance with this protection profile. For example the establishment of the time reference may use:

- a clock located in the controlled environment of the time-stamping system guaranteeing the required accuracy during the time-stamping units life-cycle (e.g. atomic clock),
- an authenticated external time source (accessible via NTP protocol and a VPN connection for example),
- three or more not authenticated external time sources of different natures (NTP servers, radio sources,...) whose values are combined using a decision algorithm (by majority vote in case of an odd number of sources for example).

The monitoring of the internal clock drift relies on:

- the comparison of the internal clock with the time reference in order to detect the important instantaneous gap between these two values,
- the checking of the internal clock synchronization using a history of gaps between the internal clock and the time reference in order to detect slow variations of the gap between these two values.

1.3 Constraints for security targets

To cover various scenarios and usage constraints, few elements are defined as parameters in this protection profile. These parameters, which will have to be specified in the products security target claiming conformance with the protection profile, are as follows:

- the guaranteed accuracy of the time contained in the time-stamp token with the UTC time,

- the manner of establishing the time reference,
- the operating duration in autonomous mode, i.e. the period of time guaranteed during which the TOE is able to function without being able to determine the time reference (this period of time depends on the drift of the internal clock of the unit - it can be null),
- the operating duration in case of temporary power failure, i.e. the period of time guaranteed during which the TOE remains in a secure operational state (this time depends on the backup duration on the internal power - it can be null),
- the frequency of the comparisons between the internal clock and the time reference, insofar as the time reference is available,
- the frequency of the update of the history of gaps between the internal clock and the time reference, insofar as the time reference is available,
- the frequency of the verification of the synchronization of the internal clock for its possible synchronization which exploits the history of the variations,
- the supported cryptographic algorithms and their parameters, including key lengths.

1.4 Definitions

A glossary giving the main terms definition used in this document is available in Appendix A.

1.5 Abbreviations

For the purposes of the present document, the following abbreviations apply:

CA	Certification Authority
CC	Common Criteria
EAL	Evaluation Assurance Level
IT	Information Technology
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
ST	Security Target
TOE	Target Of Evaluation
TSF	TOE Security Functionality
TSU	Time-Stamping Unit
UTC	Coordinated Universal Time

1.6 Associated documents

[PH]	Politiques d'horodatage – Politique de niveau standard, v0.1, 26 september 2003
[ETSI TS1]	ETSI TS 101 861: Time stamping profile, v1.2.1, March 2002
[ETSI TS2]	ETSI TS 102 023: Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities, v1.2.1, January 2001
[ITU-R]	ITU-R Recommendation TF.460-5: "Standard-Frequency and Time-signal emissions", 1997

1.7 References

[CC1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1, Revision 1, September 2006.
[CC2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements. Version 3.1, Revision 2, September 2007.
[CC3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements. Version 3.1, Revision 2, September 2007.
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology. Version 3.1, Revision 2, September 2007.
[QUA-STD]	Processus de qualification d'un produit de sécurité – Niveau standard. Version 1.1, 18 march 2008. N°549/SGDN/DCSSI/SDR.
[CRYPTO-STD]	Cryptographic mechanisms – Rules and recommendations about the choice and the parameter's sizes of cryptographic mechanisms with standard robustness level. DCSSI. http://www.ssi.gouv.fr/fr/sciences/publications.html
[AUTH-STD]	Authentification - Règles and recommandations concernant les mécanismes d'authentification de niveau de robustesse *standard*. DCSSI. http://www.ssi.gouv.fr/fr/sciences/publications.html
[KEYS-STD]	Gestion de clés - Règles and recommandations concernant la gestion des clés utilisées dans les mécanismes cryptographiques de niveau de robustesse *standard*. DCSSI. http://www.ssi.gouv.fr/fr/sciences/publications.html

2 TOE description

2.1 TOE features

The main functionality of the TOE is the time-stamp token generation, which includes the requests management and the generation of the answers by the time-stamping system.

The secondary functionalities of the TOE are:

- the definition of the default time-stamp policy of the time-stamping system,
- the initialization of the time-stamping unit corresponding to the creation of a non operational time-stamping context. It includes the synchronization of the time-stamping unit internal clock with a time source whose accuracy is known compared to a UTC(k) source,
- the time-stamping unit certificate import which allows to create an operational time-stamping unit by moving the time-stamping context to an operational state,
- the startup (or re-starting) of the time-stamping unit,
- the interruption of the time-stamping unit,
- the termination of the operational context (associated to a time-stamping unit),
- the monitoring of the internal clock drift and the maintenance of synchronization with UTC,
- the generation of audit records and alarms,
- the detection and the reaction to attacks to the unit (e.g. by the destruction of the private keys and the termination of all the contexts).

The import and the export (backup) of the private keys of the time-stamping units are not authorized.

The renewal of certificates and the change of key pairs and certificates of time-stamping contexts are not mandatory functionalities and are thus not covered by this protection profile.

The accuracy of the time-stamping unit internal clock being a parameter of this protection profile, the programming of the second jumps is consequently not considered as a mandatory functionality of the TOE.

2.1.1 Services provided by the TOE

Time-stamp token generation

The main service provided by the time-stamping system is the time-stamp token generation. These tokens correspond to the signed association of a digest of a document, of the time and hour of the time-stamping unit internal clock, of the reference of the time-stamping unit certificate, and of the applied time-stamp policy.

The logical interface of the time-stamping system allows to receive time-stamp tokens requests which must contain the digest of the document to be time-stamped, the reference to the hash function to be used and optionally the identifier of the required time-stamp policy and a nonce. When the identifier of the time-stamp policy is not specified in the request, a default time-stamp policy is applied. The time-stamping system processing the token request must verify that the hash function referred in the request is authorized by the

used time-stamp policy and that the length of the digest is adequate for the required algorithm.

If the time-stamping unit supports the requested policy or if a default policy is created in the system (i.e. the reference of the requested policy or a default policy is present in the operational time-stamping context associated with the unit), the unit generates the time-stamp tokens. The protocol must ensure that the answer corresponds to the request which has just been received.

2.1.2 Services required by the TOE

Default time-stamp policy definition

If the time-stamp token request does not specify any time-stamp policy, the default time-stamp policy must be used. For this purpose, the time-stamping system security administrator must define a default time-stamp policy with an identifier of time-stamp policy and the hash algorithms authorized for this policy.

Time-stamping unit initialization

The initialization of a time-stamping unit consists in generating the key pairs that will be used for each time-stamping context, in synchronizing the internal clock with UTC, in defining the supported time-stamp policies, in defining the hash algorithms authorized for each time-stamp policy, and in defining the validity period of the private key. The initialization process requires the presence of the security Administrator. The initial tuning of the clock and the keys generation can be performed in an unspecified order.

Initialization starts with the creation of a non operational time-stamping context which includes the following information:

1. the identification of the internal clock that shall be used to obtain the time value contained in time-stamp tokens
2. the accuracy with UTC time that is guaranteed for the time contained in time-stamp tokens,
3. the key pair value (and the identifier of the algorithm),
4. the private key validity period,
5. the reference(s) of supported time-stamp policies,
6. the identifier(s) of hash algorithms for each time-stamp policy.

At the end of this phase, the internal clock is maintained synchronized using only its synchronization algorithm and previous information are not individually modifiable and can be only globally deleted. This information is used to make a request for time-stamping unit certificate to a Certification Authority for this non operational time-stamping context.

Certificates Importation

It must be possible to associate a public-key certificate with a non operational context. At the end of this operation, the context becomes operational if the public-key contained in the certificate corresponds to the public-key already present in the context. This operation requires the presence of the Security administrator.

Concerning the effective validity period of the private key:

1. If the certificate contains an extension allowing knowing the private key validity period, the private key validity period which had been introduced during the initialization phase is ignored, and the value contained in the extension is taken into account as the effective private key validity period.
2. If the certificate does not contain an extension allowing knowing the private key validity period, the private key validity period which had been introduced during the initialization phase is taken into account as the effective validity period of the private key.

Startup and restarting

The restarting of a time-stamping unit in the event of power failure is automatic if all the synchronization and security conditions are met during the resumption of the power supply. Otherwise, the re-starting requires the presence of the security Administrator.

The restarting of a time-stamping unit in the event of automatic stop is possible when the associated operational context was not definitively stopped (following attack detection for example). The restarting requires in this case the presence of the security Administrator.

Moreover, it must also be possible to start or re-start the time-stamping during its normal life. This operation has to be able to be performed by an Operator.

Time-stamping unit interruption

The following events cause the automatic interruption of the time-stamping unit:

- power failure,
- instantaneous gap between the internal clock of the time-stamping unit and the time reference greater than an authorized value,
- history of the gap between the internal clock of the time-stamping unit and the time reference not compliant with authorized drift over a specified period of time.

Moreover, it must also be possible to temporarily stop the time-stamping unit during its normal life. This operation has to be able to be performed by an Operator.

Context termination

The termination of a context generally corresponds to the end of the context private key validity. At the end of its validity period, the context private key is automatically destroyed.

The context termination can also result from attack detection on the time-stamping system which must lead to the destruction of all the private keys of the various contexts.

The termination of a context can finally be carried out on request of the security Administrator.

Internal clocks synchronization with UTC

This service ensures the monitoring of the internal clocks drift of time-stamping unit and their synchronization with UTC.

The synchronization of the internal clock with UTC relies on:

- the initial synchronization of the internal clock during the time-stamping unit initialization with a time source whose accuracy is known compared to a UTC(k) source,
- the monitoring of the internal clock drift and the maintenance of synchronization with the time reference during the operation of the time-stamping unit.

The monitoring of the internal clock drift with the time reference relies on:

- the comparison of the internal clock with the time reference in order to detect important instantaneous gap between these two values,
- the control of the internal clock synchronization using an history of the gap between the internal clock and the time reference in order to detect slow variations of the gap between these two values.

Audit records and alarms generation

This service monitors and traces all the operations relating to the time-stamping units administration and the maintenance of the internal clocks synchronization with UTC. This service also allows the Auditor to define the events to be traced and to consult them.

Security alarms are generated in the following cases:

- attacks detection on the time-stamping units,
- instantaneous gap between the time-stamping unit internal clock and the time reference greater than an authorized value,
- history of the variations non-compliant with authorized drift over a specified period of time,
- repeated synchronizations of the time-stamping unit internal clock,
- the internal power of a time-stamping unit internal clock is outside the range of normal functioning in the event of power failure.

Attacks Detection

This service allows reacting to attacks on the time-stamping system targeting the disclosure of the private keys of the time-stamping units or the unauthorized modification of the internal clocks. In the event of attacks detection, the private keys of the various contexts must be automatically destroyed.

2.1.3 Roles

The following roles are involved in the operation of the TOE and its operational environment.

Security Administrator

Local Security Administrator of the time-stamping system: this role is to define the default time-stamp policy of the time-stamping system, to initialize the time-stamping units, and to restart them in the event of automatic stop for which an automatic restarting is not possible for security reasons.

Auditor

Administrator of the audit policy: this role is to define the events to be traced and to analyze the audit records concerning the administration of time-stamping units and synchronizations of internal clocks.

Operator

Operator of time-stamping system: this role is to ensure the normal operation of the time-stamping system as long as the security conditions remain in operation (by ensuring for example the re-starting following a power failure). He is responsible for the maintenance in operational condition of the TOE.

User

User of the time-stamping system: this role is to send requests containing digest of documents to time-stamp and the identifier of the hash function used to obtain the digest. It must also verify the validity of the delivered time-stamp token and ensure that the time-stamping unit certificate is valid and was not revoked.

Supervisor

Supervisor (local or remote) of the time-stamping system: this role is to verify the normal operation of the time-stamping system. The supervision of the time-stamping system can be performed remotely.

Thereafter, the **Administrator** role comprises the roles **security Administrator** and **Auditor**.

2.2 TOE boundaries

This section describes what is included in the TOE, which will thus be evaluated, of what belongs to its operational environment.

2.2.1 Physical scope

Figure 1 presents an example of physical environment possible for the TOE and the possible interactions during the operation of a time-stamping unit. The use of UTC time sources is not necessarily required after the time-stamping unit initialization.

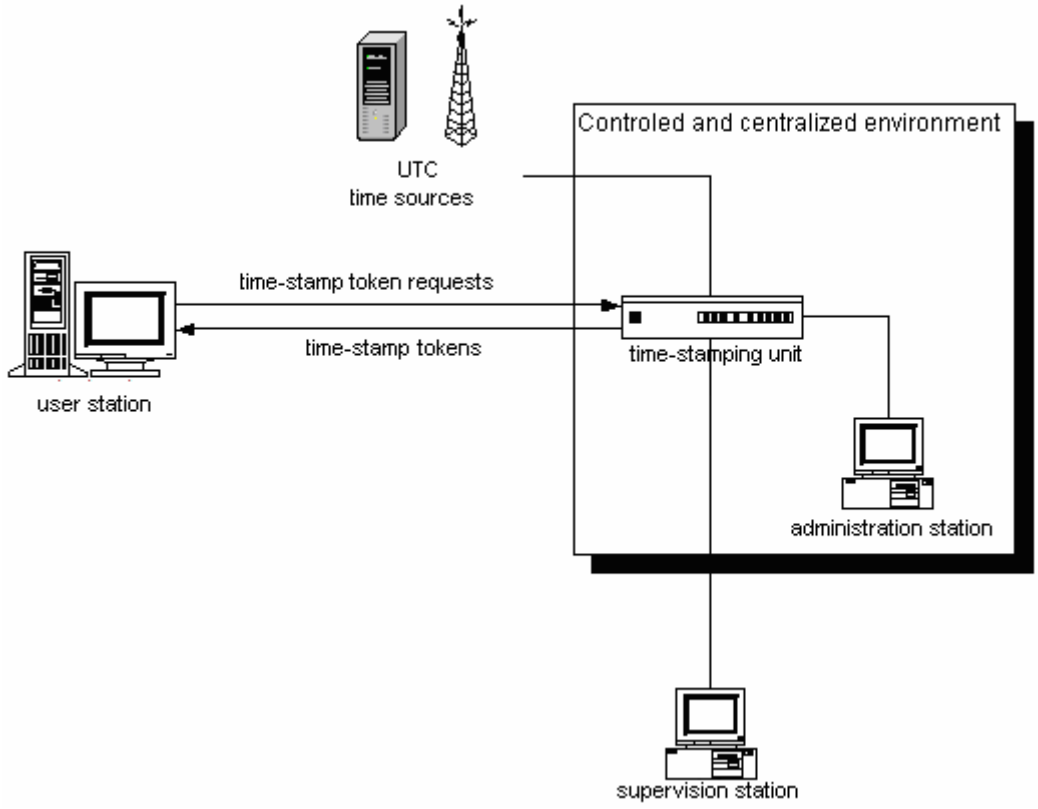

Figure1. Example of TOE architecture and its environment

2.2.2 Logical scope

Figure 2 details the functional components which compose the TOE at the logical level. The TOE functional boundaries are defined by the grayed components.

The local authentication of the Security Administrator and of the Auditor on a time-stamping unit belongs to the TOE boundaries.

The supervision functions and the supervision station itself are not considered in the TOE boundaries.

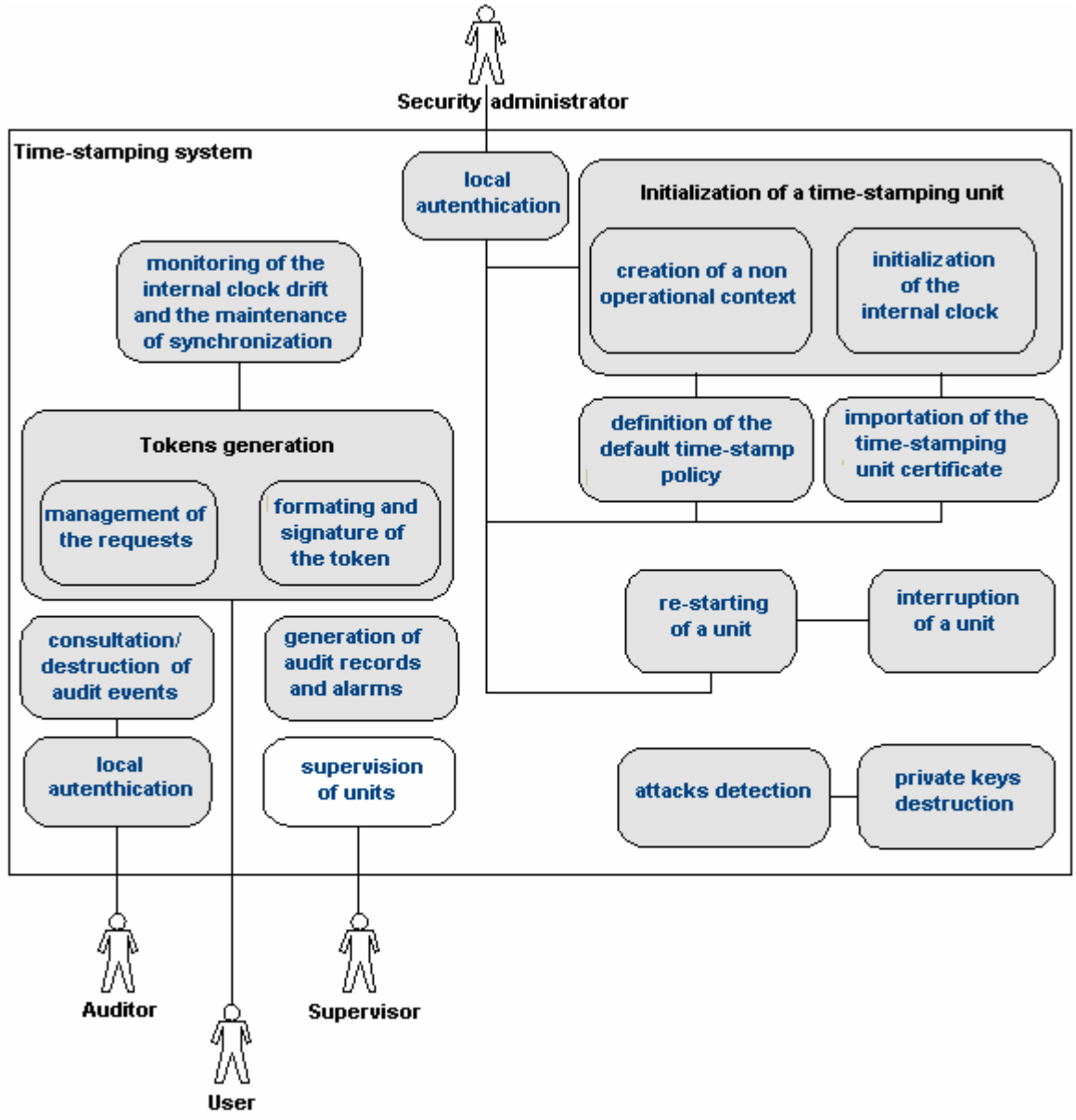

Figure2. Logical view of the time-stamping system

The audit of the time-stamping transactions and the access to these transactions by an Administrator are not included in the TOE boundaries.

2.3 TOE operational environment

For the security of the TOE, the time-stamping units and the administration equipment must be in a secure place and their accesses must be controlled. A supervision of the time-stamping system is possible via a remote workstation but this one is not included in the TOE boundaries.

Application note

If the time-stamping system allows a remote administration, the product can claim conformance with this PP but the security target must comprise the threats, assumptions, OSP, security objectives and security requirements relating to the remote administration

operations. In this case, the assumption on local administration A.LOCAL_ADMIN must be replaced by a threat relating to the remote administration.

3 Conformance claims

This chapter contains the following sections:

CC conformance claim (3.1)

Package claim (3.2)

PP claim (3.3)

Conformance statement (3.4)

3.1 CC conformance claim

This protection profile claims strict conformance with the Common Criteria version 3.1.

It was written in accordance with:

- CC Part 1 [CC1],
- CC Part 2 [CC2],
- CC Part 3 [CC3],
- and the CC evaluation methodology [CEM].

3.2 Package claim

This PP is in conformance with the assurance requirements package defined by the DCSSI *standard qualification* process [QUA-STD].

3.3 PP claim

This PP does not claim conformance with any other PP.

3.4 Conformance statement

The conformance required for the Security Targets and Protection Profiles which claim conformance with this Protection Profile is **demonstrable** according to the definition in CC Part 1 [CC1].

4 Security problem definition

4.1 Assets

The description of each asset provides the security features which must be applied to counter the threats or cover the OSPs related to this asset described further in this document (*Protection* statement).

4.1.1 User data

4.1.1.1 Time-stamping token requests

D.REQUEST

This asset is the request sent to the time-stamping system for the generation of a time-stamp token. It must contain the following information:

- the digest of the document to time-stamp,
- the identifier of the hash algorithm used to generate this digest.

It can also (optionally) contain the identifier of a specifically-requested time-stamp policy and a nonce. This nonce, if present in the request, allows the User of the time-stamping system to check that the answer delivered by the system corresponds to the request delivered in the absence of User local clock. The digest of the document corresponds to the result of the application to the document to time-stamp of a hash algorithm which must be authorized by the requested time-stamp policy. The time-stamping system interface allows passing only the digest of a document, and not the document itself.

Protection: integrity.

4.1.1.2 Time-stamp tokens

D.TOKEN

The time-stamp token corresponds to the association of a document digest and a UTC time mark. The token is signed by the valid private key of the time-stamping unit operational context.

Protection: integrity and authentication of origin.

4.1.2 TSF data

4.1.2.1 Time-stamping contexts

D.NON_OPERATIONAL_CONTEXT

This asset corresponds to the association of the following information:

- identification of the internal clock used to obtain the time value contained in the time-stamp token,
- the accuracy with UTC time that is guaranteed for the time contained in time-stamp token,
- the key pair value (and the identifier of the algorithm),

- the private key validity period,
- reference(s) of supported time-stamp policies,
- identifiers of authorized hash algorithms for each time-stamp policy.

Protection: integrity.

Application note

A time-stamping unit can contain several non operational contexts but cannot contain more than one operational context at the same moment.

4.1.2.2 Internal clock

D.TIME_REFERENCE

This asset represents a local approximation of the UTC time calculated at some given instant of time.

Protection: integrity.

Application note

The time reference allows ensuring the monitoring of the drift and the synchronization of the time-stamping unit internal clock. It is used:

- during the comparison of the internal clock with the time reference,
- during the verification of the synchronization of the internal clock for its possible synchronization which exploits the history of the gap between the internal clock and the time reference.

D.INTERNAL_CLOCK

This asset represents the time-stamping unit internal clock which provides the date and the hour corresponding to UTC time being used to time-stamp the tokens.

Protection: synchronization with UTC.

Application note

A time-stamping system can comprise several time-stamping units using each one a specific internal clock. The clocks of the various time-stamping units can have different accuracy guaranteed with UTC.

D.TIME_GAP_HISTORY

This asset represents the history of the gap between the time-stamping unit internal clock and the time reference.

Protection: integrity.

Application note

This history is exploited by an algorithm of synchronization which must deduce if a resynchronization of the internal clock is necessary or if a stop of the time-stamp tokens generation service is necessary in the event of evolution of gaps too important for a specified period of time.

In the event of interruption of the time-stamp tokens generation service, it is recommended to continue to upgrade the history until the intervention of the Auditor.

4.1.2.3 Time-stamp policy

D.ID_POLICIES

The identifiers of time-stamp policies are defined during the creation phase of a non-operational context. They allow to refer the applicable rules by the TOE and its environment.

Protection: integrity.

Application note

Several non-operational contexts being able to support different time-stamp policies can be created in the time-stamping system.

D.ID_HASH_FUNCTION

The identifiers of the authorized hash algorithms allow to determine the functions used to generate the digest to time-stamp. They must be defined for each time-stamp policy and are associated with a digest length which must be checked by the time-stamping unit managing the time-stamp token requests.

Protection: integrity.

4.1.2.4 Cryptographic keys

D.CERTIFICATE

This asset corresponds to the public key certificate associated with the private key of the signature used by an operational context. The public-key value contained in the certificate must correspond to the public-key generated during the creation of the non operational context. The certificate is signed by a Certification Authority.

Protection: integrity and authentication of origin.

Application note

Several operational contexts can be present in the time-stamping system. Indeed, the import and the export of time-stamping unit private keys not being authorized, it necessarily exists several time-stamping contexts if several time-stamping units are present in the system.

D.SIGNATURE_PRIVATE_KEY

This asset represents the private key of a time-stamping context which can be used to sign the time-stamp tokens when the context is operational.

Protection: confidentiality and integrity.

Application note

Several private keys corresponding to various time-stamping contexts can be present in the time-stamping system.

D.INITIAL_PRIVATE_KEY_VALIDITY_PERIOD

This asset represents the private key validity period which is defined during the creation of a non operational context by the Security administrator.

Protection: integrity.

D.EFFECTIVE_PRIVATE_KEY_VALIDITY_PERIOD

This asset represents the effective private key validity period of an operational context. Two cases are implemented:

1. if the time-stamping unit certificate contains an extension allowing to know the private key validity period, private key validity period which had been introduced during the initialization phase is ignored, and the value contained in the extension is taken into account,

2. if the time-stamping unit certificate does not contain an extension allowing to know the private key validity period, private key validity period which had been introduced during the initialization phase is taken into account.

Protection: integrity.

D.SIGNATURE_PUBLIC_KEY

This asset represents the public-key generated during the creation of a non operational time-stamping context.

Protection: integrity.

Application note

Several public-keys corresponding to various time-stamping contexts can be present in the time-stamping system.

D.ADMIN_AUTH_DATA

This asset represents the authentication data used by the administrators to authenticate themselves on the TOE.

Protection: confidentiality and integrity.

4.1.2.5 Time-stamping unit status

D.POWER_STATE

This asset allows determining the power state of a time-stamping unit:

- in operation using an external power supply,
- internal clock maintained using an internal power supply with the time-stamping unit in a range of normal functioning (following a power failure),
- internal clock maintained using an internal power supply with the time-stamping unit out of the range of normal functioning (insufficient power level to maintain the protection of the keys and the clock).

Protection: integrity.

Application note

Several time-stamping units can be present in the time-stamping system.

D.SYNCHRO_STATE

This asset allows to know the current state of synchronization of the time-stamping unit internal clock.

Protection: integrity.

Application note

Several time-stamping units can be present in the time-stamping system.

4.1.2.6 Audit and alarms

D.AUDIT_RECORDS

This asset corresponds to the audit records associated with the TOE administration and with the control and synchronizations of the time-stamping unit internal clock. The audit records relating to the control and the internal clock synchronization concern:

- the date and the value of the last correct comparison between the internal clock and the time reference in order to, if necessary, being able to detect an incident during the control of following synchronization with the time reference,
- the date and the value of internal clock synchronizations.

Protection: integrity and availability.

Application note

Several time-stamping units can be present in the time-stamping system.

D.ALARMS

This asset corresponds to the security alarms sent by the time-stamping unit to the Security Administrator and the Auditor. Alarms are generated in the following cases:

- attacks detection on a time-stamping unit,
- repeated synchronizations of the time-stamping unit internal clock,
- instantaneous gap between the time-stamping unit internal clock and the time reference greater than an authorized value,
- historical of the gaps non-compliant with the drift authorized over a specified period of time,
- the internal power of a time-stamping unit internal clock is outside the range of normal functioning in the event of external power failure.

Protection: integrity and availability.

Application note

Several time-stamping units can be present in the time-stamping system.

4.2 Threats

The DCSSI *standard qualification* process applies to consumers products ensuring the protection of information with restricted diffusion. Consequently, few threats are not taken into account in this protection profile such as for example, the theft of the equipment (which will have to be detected by organisational measurements), or the denial-of-service. The threats present in this section are only threats which violate the TOE security and not the services provided by the TOE, because all the environment elements concerning the services returned by the TOE are considered as organisational security policies.

The threat agents are:

- Internal attackers: any person authorized to access the controlled environment of the TOE (Operators for example), except for the administrators (security administrators and auditors) who are considered trusted (assumptions A.ADMIN).
- External attackers: any person external with the controlled environment of the TOE (Users of the time-stamping service for example).

4.2.1 Threats on time-stamping contexts

T.CONTEXT_MODIFICATION

An internal attacker modifies in an unauthorized way the following information belonging to a time-stamping context:

- o the identification of the internal clock in order to use a less accurate internal clock,
- o the accuracy with UTC time that is guaranteed for the time contained in the time-stamp token in order to improve the accuracy which can be indicated in the time-stamp token,
- o the private key value in order to create a denial-of-service situation,
- o the public-key value in order to make certify a public-key whose private key is known or to create a denial-of-service situation,
- o the private key validity period defined in the context creation in order to preserve the private key for a period longer than the one initially envisaged,
- o the effective private key validity period in order to preserve the private key for a period duration longer than the one calculated at the end of the time-stamping unit initialization,
- o the reference(s) of the time-stamp policies supported in order to refer policies which guarantee a better clock accuracy than the one of the internal clock used or which authorize weaker hash algorithms,
- o the identifiers of the hash algorithms for each time-stamp policy in order to refer weaker hash algorithms,
- o the time-stamping unit certificate in order to deliver a certificate with a private key validity period or a private key validity period longer, or to create a denial-of-service situation.

4.2.2 Threats on internal clock

T.CLOCK_MODIFICATION

An internal attacker modifies the time-stamping unit internal clock in order to obtain predated or postdated tokens generated with a time reference whose variation with UTC does not satisfy the accuracy required by the time-stamp policy.

This modification may result:

- o from a direct attack on the time-stamping unit internal clock,
- o from an indirect attack on the internal clock by modifying the time reference which will be taken into account in the history of the gaps exploited for the resynchronization of the internal clock.

T.TIME_GAP_HISTORY_MODIFICATION

An internal attacker modifies the history of the gap between the time-stamping unit internal clock and the time reference so that an internal clock drift is neither detected nor taken into account during the synchronization verification.

4.2.3 Threats on time-stamp token requests

T.REQUEST_FORGERY

An external attacker compromises the integrity of the services or of the sensitive assets of the TOE by forging malformed requests to the time-stamping system.

T.INCOHERENT_HASH

An external attacker provides by modifying a time-stamp token request:

- a digest whose length is incoherent with the referred hash algorithm, or
- an identifier of a hash algorithm which is not authorized by the time-stamp policy specified in the request, or, when this identifier is not specified, which is not authorized by the default policy.

4.2.4 Threats on cryptographic keys

T.KEYS_DISCLOSURE

An internal attacker succeeds to access to the time-stamping unit private key and disclose it in order:

- to usurp the identity of this time-stamping unit during a later generation of tokens, or
- to compromise tokens previously generated with this unit.

T.ADMIN_AUTH_DATA_DISCLOSURE

An internal attacker succeeds to access the authentication data used by the security Administrator or the Auditor and disclose them allowing an unauthorized person to authenticate itself on the TOE.

T.ADMIN_AUTH_DATA_MODIFICATION

An internal attacker modifies the authentication data used by the Security Administrator or the Auditor to create a denial-of-service situation for the administration or auditing operations, or to disclose them to a person who can thus authenticate itself on the TOE in an unauthorized way.

4.2.5 Threats on time-stamping unit status

T.POWER_STATE_MODIFICATION

An internal attacker modifies the power state of a time-stamping unit to maintain the generation of tokens services in spite of a power failure, or to prevent the destruction of the time-stamping contexts when the time-stamping unit internal power supply is outside of its normal functioning range.

T.SYNCHRO_STATE_MODIFICATION

An internal attacker modifies the current state of synchronization of the time-stamping unit internal clock to maintain the generation of tokens services with a time reference whose variation with UTC does not satisfy the accuracy required by the time-stamp policy.

4.2.6 Threats on administration operations

T.ADMIN_USURPATION

An internal attacker pretends to be a Security Administrator or an Auditor and performs unauthorized administration or auditing operations.

4.2.7 Threats on audit records

T.AUDIT_RECORDS_MODIFICATION

An internal attacker modifies the audit records in order to delete illicit operations performed on the time-stamping system.

4.3 Organisational Security Policy (OSP)

The organisational security policies present in this section are only related to the expected functions of the TOE and therefore only concern the services provided by the TOE.

OSP.SERVICES

The TOE must generate time-stamp tokens in accordance with a specified time-stamp policy. The time-stamp tokens are signed by the private key of the time-stamping unit operational context. The tokens must at least include the following elements:

- o the digest of the document and the identifier of the hash algorithm used to generate it,
- o the time provided by the time-stamping unit internal clock used whose accuracy with UTC time is guaranteed,
- o the non ambiguous reference of the time-stamping unit certificate,
- o the reference of the applied time-stamp policy.

OSP.CRYPTO

The DCSSI cryptographic requirements [CRYPTO-STD], [KEYS-STD] and [AUTH-STD] must be followed for the cryptographic functions used in the TOE and for cryptographic key management and authentication data of the TOE (identification and authentication of the administrators, key pairs generation, private keys destruction, and signature generation for the time-stamp tokens).

OSP.INTERNAL_CLOCK_SYNCHRONIZATION

The TOE must ensure the monitoring of the drift of the time-stamping unit internal clock and the maintenance of its synchronization compared to UTC time during the operation of the time-stamping unit. The synchronization of the internal clock is carried out using an algorithm of synchronization exploiting a history of the gap between this internal clock and the time reference.

OSP.DEFAULT_POLICY

The TOE must allow defining a default time-stamp policy and the identifiers of the hash algorithms authorized by this policy. This default time-stamp policy is used when the time-stamp tokens request does not contain an identifier of the applicable time-stamp policy.

OSP.CONTEXT_MANAGEMENT

The TOE must allow:

- o the creation by the Security Administrator of non operational time-stamp contexts,
- o the consultation by the Security Administrator of the information defined in the time-stamping contexts except for the private keys values of the various contexts,
- o the termination by the Security Administrator and the TOE of time-stamping contexts.

OSP.CERTIFICATE_IMPORTATION

The TOE must allow importing the certificate corresponding to the key pair of a non operational context. The public-key appearing in the certificate must correspond to the public-key already present in the context.

OSP.REQUEST_PROTOCOL

The protocol implemented by the TOE for the management of the time-stamp tokens requests must guarantee the presence of the data elements of the request in the answer delivered by the time-stamping system. These elements include the identifier of the hash algorithm used to obtain the digest of the document, the value of the digest itself and, in an optional way, the identifier of the time-stamp policy required and a nonce.

The nonce, if it is present in the request, allows the User of the time-stamping system to verify that the answer delivered by the system corresponds to the request delivered in the absence of local clock in the User environment.

4.4 Assumptions

4.4.1 Assumptions on TOE usage

A.TOKEN_VERIFICATION

It is supposed that the user of the TOE main service validates and preserves the time-stamp tokens delivered by the time-stamping system. The token validation includes the verification:

- o of the token signature,
- o of the validity of the time-stamping unit certificate,
- o of the correspondence of the time-stamped digest with the digest transmitted in the request.

A.ADMIN

The administrators are trusted and qualified people who have the necessary means to the realization of their tasks. They are trained to execute the operations for which they have the responsibility and follow the guidance and procedures of administration which include the maintenance of the time-stamping system.

A.AUDIT

It is supposed that the auditor consults regularly the audit records generated by the TOE. It is also supposed that the memory containing the audit records is managed in such a way that the auditor does not lose records.

4.4.2 Assumptions on the TOE operational environment

A.CERTIFICATION_AUTHORITY

It is supposed that the Certification Authorities issuing the time-stamping units certificates implement practices in accordance with a certification policy approved by the time-stamping authority. These practices cover the activities relating to the delivery and the revocation of these certificates.

A.TIME_STAMPING_AUTHORITY

It is supposed that the time-stamping authority which is responsible for the time-stamping service provided by the TOE satisfies the rules defined by the time-stamp policies specified in the time-stamping contexts.

A.TIME_REFERENCE

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

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.LOCATION

The equipment constituting the TOE must be in secure buildings with access controlled in order to prevent any unauthorized physical access.

A.LOCAL_ADMIN

It is supposed that the TOE administration is performed locally from the secure environment where the TOE is located.

A.NETWORK

It is supposed that the network on which the TOE is connected is deployed and managed in accordance with a network interconnection policy ensuring the filtering of entering flows.

A.SUPERVISION

It is supposed that the TOE environment allows remote supervision of the operational state of the time-stamping system.

5 Security objectives

5.1 Security objectives for the TOE

5.1.1 Security objectives on services provided by the TOE

O.REQUEST_PROTOCOL

The TOE shall implement a management protocol of the time-stamp tokens requests guaranteeing that the answers delivered by the time-stamping system contain the data elements present in the corresponding requests. These elements include the identifier of the hash algorithm used to obtain the digest of the document, the value of the digest itself and, in an optional way, the identifier of the time-stamp policy required and a nonce.

O.TOKEN_GENERATION

The TOE shall guarantee the integrity and the authentication of the tokens origin during their delivery by the time-stamping system. The generated time-stamp tokens must at least include the following elements:

- the digest of the document and the identifier of the hash algorithm used to generate it,
- the time provided by the time-stamping unit internal clock used whose accuracy with UTC time is guaranteed,
- the non ambiguous reference of the time-stamping unit certificate,
- the reference(s) of the applied time-stamp policy.

Before signing a time-stamp token, the TOE must also guarantee that the time (date and hour) which must be included is in no case earlier than the time which was included in the token previously delivered by the time-stamping unit.

5.1.2 Security objectives to protect TSF data

5.1.2.1 Time-stamp tokens request management

O.REQUEST_VERIFICATION

The TOE shall check the conformance of the time-stamp tokens requests with respect to the awaited format.

O.HASH_VERIFICATION

The TOE shall check, during a time-stamping token request, that the digest length of the document to time-stamp is coherent with the identifier of the referred hash algorithm, and that this algorithm is authorized by the time-stamp policy.

O.DEFAULT_POLICY

The TOE shall allow defining the default time-stamp policy and the identifiers of the hash algorithms authorized by this policy.

5.1.2.2 Time-stamping contexts management

O.NON_OPERATIONAL_CONTEXT_CREATION

The TOE shall allow the Security administrator to create a non operational time-stamping context which includes the following information:

- the identification of the internal clock that shall be used to obtain the time value contained in the time-stamp token,
- the accuracy with UTC time that is guaranteed for the time contained in the time-stamp tokens,
- the key pair value (and the identifier of the public key algorithm) for the creation and the verification of the time-stamp tokens signature,
- the private key validity period,
- the reference(s) of the supported time-stamp policies,
- the identifiers of the hash algorithms for each time-stamp policy.

All information, except the key pair value, can be modified by the Security Administrator as long as the non operational time-stamping context is not declared as created by the Security Administrator. Information of a non operational time-stamping context declared as created is not modifiable individually and can only be completely deleted by the Security Administrator.

O.OPERATIONAL_CONTEXT_PROTECTION

The TOE shall guarantee that an operational time-stamping context cannot be modified. On the other hand, an operational time-stamping context can be definitively stopped, which involves the destruction of the private key of this context.

O.CONTEXTS_VISUALIZATION

The TOE shall allow the Security Administrator to visualize the following information contained in the time-stamping contexts supported by the time-stamping system:

- the identification of the internal clock that shall be used to obtain the time value contained in the time-stamp token,
- the accuracy with UTC time that is guaranteed for the time contained in time-stamp tokens,
- the private key validity period defined during the time-stamping unit initialization,
- the reference(s) of the supported time-stamp policies,
- the identifiers of the hash algorithms for each time-stamp policy,
- the effective private key validity period of the context (for the operational contexts),
- the time-stamping unit certificate (for the operational contexts).

O.CONTEXT_STOP

The TOE shall be able to stop a time-stamping context definitively and to cease using information of this context to provide the services of time-stamp tokens generation in the following cases:

- attacks detection on the time-stamping system (causing the termination of all the contexts),

- o the internal power supply of the time-stamping unit is outside the range of normal functioning (insufficient power level to maintain the protection of the keys and the clock),
- o on request of the Security administrator.

The termination of a context must involve the destruction of the associated private key.

5.1.2.3 Synchronization Management

O.INTERNAL_CLOCK

The TOE shall ensure the synchronization of the time-stamping unit internal clocks with UTC with the accuracy required by the time-stamp policy. The synchronization of the time-stamping unit internal clock is performed using an algorithm of synchronization exploiting a history of the gap between this internal clock and the time reference.

Application note

When the required accuracy is lower or equal to the second, the second jumps should be programmed in advance and a programming omission should cause the interruption of the time-stamping unit.

5.1.2.4 Cryptographic keys management

O.CRYPTO

The TOE shall implement cryptographic functions and manage cryptographic keys and authentication data in conformance with the DCSSI cryptographic requirements [CRYPTO-STD], [KEYS-STD] and [AUTH-STD]. Cryptographic keys management and authentication data concerns:

- o the identification and authentication of the administrators,
- o the key pairs generation used to create and verify the signature of the time-stamp tokens delivered by the time-stamping system,
- o the destruction of the private keys of the time-stamping contexts,
- o the generation of signature for the time-stamp tokens.

O.CERTIFICATE_IMPORTATION

The TOE shall allow importing the public-key certificate corresponding to the key pair of a non operational context provided that the public-key present in the certificate corresponds to the public-key already present in this context.

O.KEYS_EXPORT

The TOE shall not allow exporting the signature private keys generated by the TOE.

O.KEYS_IMPORT

The TOE shall not allow importing signature private keys or signature keys pairs generated outside of the TOE.

5.1.2.5 Time-stamping unit interruption

O.INTERRUPTION

The TOE shall stop to generate time-stamping tokens in the following cases:

- the current state of synchronization of the time-stamping unit internal clock does not allow to guarantee the accuracy required by the time-stamp policy (the instantaneous gap between the internal clock and the time reference is greater than a threshold or the history of the gaps between the internal clock and the time reference does not conform to the drift authorized for a specified period of time),
- the internal clock uses the internal power supply (following a failure of the external power supply).

This stop is temporary and does not lead to the termination of the operational time-stamping context.

O.SECURE_STATE_RETURN

The TOE shall provide a functionality allowing the time-stamping unit to return in a secure operational state following an interruption.

5.1.2.6 Administration

O.ADMIN_AUTHENTICATION

The TOE shall provide identification and authentication mechanisms for the Administrators.

5.1.2.7 Audit and alarms

O.TIMESTAMPING_UNIT_LOGS

The TOE shall trace all the operations performed on the time-stamping units related to the management of the time-stamping contexts and the synchronization of the internal clocks of the time-stamping units. Moreover, the TOE shall allow the Auditor to consult the audit records. The audit records relating to the synchronization of the time-stamping unit internal clock concern:

- the synchronization control operations necessary to preserve the date and the value of the last correct comparison between the internal clock and the time reference,
- synchronization operations necessary to preserve the date and the value of synchronizations of the internal clock.

Application note

The trace of the synchronization control operations is used to determine from which date the tokens with a wrong UTC time would have been delivered. The trace of the synchronization operations is used to identify when the time-stamping unit internal clock have been resynchronized.

O.ADMINISTRATION_LOGS

The TOE shall trace all the operations performed by the Security administrator on the time-stamping system. Moreover, it shall allow the Auditor to consult the audit records.

O.AUDIT_RECORDS_PROTECTION

The TOE shall guarantee the integrity and the availability of the audit records.

O.ALARMS

The TOE shall generate security alarms for any potential violation of security, in particular in the following cases:

- repeated synchronizations of the time-stamping unit internal clock,
- the memory used to store the audit records is close to its maximum capacity,
- the instantaneous gap between the internal clock and the time reference is greater than an authorized value,
- the history of the gaps between the internal clock and the time reference is not compliant with the drift authorized for a specified period of time.

5.2 Security objectives for the operational environment

OE.TOKEN_VERIFICATION

The user of the TOE main service shall validate and preserve the time-stamp tokens delivered by the time-stamping system. The validation of the token includes the verification:

- of the token signature,
- of the validity of the time-stamping unit certificate,
- of the correspondence of the time-stamped digest with the digest transmitted in the request.

OE.ADMIN

The administrators shall be trained with the tasks which they have to realize on the TOE.

OE.LOCAL_ADMIN

The TOE administration shall be performed locally from the secure environment where the TOE is located.

OE.CERTIFICATE_REQUEST

The Security Administrator shall verify that the request to a Certification Authority for a time-stamping unit certificate contains at least the following information of the non operational context:

- the value of the public-key (and the identifier of the algorithm),
- the private key validity period,
- the reference(s) of the supported time-stamp policies.

OE.CERTIFICATE_IMPORT

The Security Administrator shall verify, during the time-stamping unit certificate importation, that it has been generated by a Certification Authority authorized to deliver certificates for the targeted context of operations.

OE.AUDIT_RECORDS_ANALYSIS

The Auditor shall regularly analyze the audit events recorded by the TOE and act consequently. Moreover, memory management containing the audit events must be made in such a way that the auditor does not lose events.

OE.TIMESTAMPING_AUTHORITY

The time-stamping authority responsible for the time-stamping service provided by the TOE shall apply the rules defined by the time-stamp policies specified in the time-stamping contexts.

OE.CERTIFICATION_AUTHORITY

The Certification Authorities delivering the certificates of the time-stamping units shall implement practices in accordance with a certification policy approved by the time-stamping authority. These practices must cover the activities relating to the delivery and the revocation of these certificates.

OE.PHYSICAL_PROTECTION

The equipments constituting the TOE shall be located in a secure room with access controlled and limited to authorized people.

OE.NETWORK

The network on which the TOE is connected shall be deployed, configured and managed in accordance with a network interconnection policy ensuring the filtering of entering flows.

OE.SUPERVISION

The TOE environment shall allow a Supervisor to remotely consult the operational state of the time-stamping system.

OE.TIME_REFERENCE

The personnel responsible for the initialization of the time-stamping units (including the Security Administrator) must proceed, during this initialization, to a verification of a correct initialization of the time reference.

Moreover, the TOE environment shall guarantee that no attack can compromise simultaneously and in a coherent way the values of a time-stamping unit internal clock and the time reference.

6 Security requirements

6.1 Security functional requirements

In the security functional requirements, the two following terms are used to design a refinement:

- *Editorial refinement* (term defined in [CC1]): refinement in which a minor modification is performed on a requirement element, such as the rewording of a sentence of a requirement from grammatical reasons. In any case, this will change the requirement meaning.
- *Refinement*: refinement which allows to add points or to limit the set of acceptable implementations for a given requirement element or for all the requirement elements of a component.

Below the list of Subjects, Objects, Operations and their Security attributes used in the formulation of the security functional requirements:

Context Management Policy

- **Subjects:** subject representing the Security Administrator (S.security_admin),
- **Operations:** creation, modification, destruction and consultation of the timestamping contexts (OP.context_creation, OP.context_modification, OP.context_destruction, and OP.context_consultation respectively),
- **Objects:** timestamping contexts (OB.timestamping_context),
- **Security attributes:**
  - the security attribute AT.context_operational associated with a timestamping context (OB.timestamping_context),
  - the security attributes AT.non_operational_context_complete and AT.non_operational_context_created associated with a timestamping context (OB.timestamping_context),

Key Management Policy

- **Subjects:** subjects that export the public key generated by the TOE and import the corresponding public key certificate of the timestamping unit into the TOE to create an operational context (S.public_key_export_module and S.timestamping_unit_certificate_import_module respectively),
- **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),
- **Information:**
  - value of the timestamping unit certificate imported into the TOE (I.imported_certificate),
  - value of the public key contained in the timestamping unit certificate imported into the TOE (I.imported_certificate_public_key),
  - value of the public key of the non operational context into which the certificate is imported (I.non_operational_context_public_key),

  - value of the private key of the non operational context into which the certificate is imported (I.non_operational_context_private_key),
  - value of the private key validity period contained in the timestamping unit certificate imported into the TOE, if present (I.imported_certificate_private_key_validity_period),
  - value of the public key algorithm identifier (I.public_key_algorithm_identifier),
- **Objects:** timestamping contexts (OB.timestamping_context),
- **Security attributes:**
  - the security attributes AT.non_operational_context_complete and AT.non_operational_context_created associated with a non operational context (OB.timestamping_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 Administrator,
  - the security attribute AT.context_operational that indicates that a timestamping context (OB.timestamping_context) is operational following the authorized import of the timestamping unit certificate,
  - the security attributes AT.private_key_initial_validity_period associated with a non operational context (OB.timestamping_context with security attribute AT.context_operational being "False") and AT.private_key_effective_validity_period associated with an operational context (OB.timestamping_context with security attribute AT.context_operational being "True") that concern the validity period of the private key of the timestamping context.

Timestamp Token Generation Policy

- **Subjects:** subjects that import timestamp token requests and exports signed timestamp tokens as responses to such requests (S.timestamp_token_request_import_module and S.timestamp_token_export_module respectively),
- **Operations:** import of timestamp token requests (OP.timestamp_token_request_import), and export of signed timestamp tokens (OP.timestamp_token_export),
- **Information:**
  - value of the imported timestamp token request (I.timestamp_token_request),
  - value of the hash algorithm identifier used to generate the data imprint contained in the imported timestamp token request (I.hash_algorithm_identifier),
  - value of the data imprint contained in the imported timestamp token request (I.data_imprint),
  - value of the timestamping policy identifier contained in the imported timestamp token request, if present (I.request_policy_identifier),
  - value of the nonce contained in the imported timestamp token request, if present (I.request_nonce),
  - value of the time contained in the exported timestamp token (I.timestamp_token_time),
  - value of the timestamping unit certificate reference (I.timestamping_unit_certificate_reference)

- value of the used timestamping policy contained in the exported timestamp token (I.used_timestamping_policy_identifier),
- value of the timestamp token signature (I.timestamp_token_signature),

- **Objects:** timestamp tokens (OB.timestamp_token)
- **Security attributes:**
  - the security attribute AT.context_operational associated with a timestamping context (OB.timestamping_context) that indicates that timestamp tokens can be generated using the information specified in this context,
  - the security attribute AT.internal_clock_synchronized associated with a timestamping context (OB.timestamping_context) 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 by an authenticated Security Administrator.

Timestamp Token Generation Policy

- **Subjects:** subject that generates signed timestamp tokens (S.timestamp_token_generation_module),
- **Objects:** operational contexts (OB.timestamping_context with security attribute AT.context_operational being "True") generating timestamp tokens signed against the context signature private key, and generated timestamp tokens (OB.timestamp_token) containing the information present in the corresponding timestamp token requests (I.timestamp_token_request), the time value provided by the used internal clock (I.timestamp_token_time), the value of the timestamping unit certificate reference (I.timestamping_unit_certificate_reference) and the value of the used timestamping policy (I.used_timestamping_policy_identifier),
- **Operations:** creation and signature of timestamp tokens (OP.timestamp_token_creation and OP.timestamp_token_signature respectively),
- **Security attributes:**
  - the security attribute AT.context_operational that indicates if the timestamping context (OB.timestamping_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.timestamping_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.internal_clock_synchronized associated with the used operational context (OB.timestamping_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 Administrator.

6.1.1 Time-stamping context management policy

FDP_ACC.1/Context_Management_Policy Subset access control

FDP_ACC.1.1/Context_Management_Policy The TSF shall enforce the **context management policy** on

- **Subjects: subject representing the Security Administrator (S.security_admin),**
- **Objects: timestamping contexts (OB.timestamping_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

FDP_ACF.1.1/Context_Management_Policy The TSF shall enforce the **context management policy** to objects based on the following:

- **the security attribute AT.context_operational associated with a timestamping context (OB.timestamping_context),**
- **the security attributes AT.non_operational_context_complete and AT.non_operational_context_created associated with a timestamping context (OB.timestamping_context)**.

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

- **The creation of a non operational context (OP.context_creation) is authorized to be performed only by an authenticated Security Administrator (S.security_admin) only if the following required information have been defined for this context (i.e., the value of the security attribute AT.non_operational_context_complete is "True"):**
  - **identification of the internal clock that shall be used to obtain the time value contained in timestamp tokens,**
  - **the accuracy with UTC time that is guaranteed for the time contained in timestamping tokens,**
  - **the private key validity period defined during the context creation phase,**
  - **reference(s) of accepted timestamping policies,**
  - **identifier(s) of authorized hash algorithms for each timestamping policy (recommendations for the choice of hash algorithms are provided in [CRYPTO-STD]).**
- **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 Administrator (S.security_admin):**

- **identification of the internal clock that shall be used to obtain the time value contained in timestamp tokens,**
- **the accuracy with UTC time that is guaranteed for the time contained in timestamping tokens,**
- **the private key validity period defined during the context creation phase,**
- **reference(s) of the accepted timestamping policies,**
- **identifiers of authorized hash algorithms for each timestamping policy,**
- **the private key effective validity period (for operational contexts only),**
- **the timestamping unit certificate (for operational contexts only).**

o **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 Administrator (S.security_admin) only if the non operational context has not yet been created (i.e., the value of the security attribute AT.non_operational_context_created associated with the non operation context is "False").**

o **The destruction of both non operational and operational contexts (OP.context_destruction) is authorized to be performed by an authenticated Security Administrator (S.security_admin)**.

FDP_ACF.1.3/Context_Management_Policy The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

o **if all the rules stated in FDP_ADF.1.4 are satisfied**.

FDP_ACF.1.4/Context_Management_Policy The TSF shall explicitly deny access of subjects to objects based on the **following rules:**

o **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,**

o **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**.

FMT_MSA.3/Context Static attribute initialisation

FMT_MSA.3.1/Context The TSF shall enforce the **following policies:**

o **context management policy,**

o **key management policy,**

o **timestamp token generation policy,** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/Context The TSF shall allow the **following role: none** to specify alternative initial values to override the default values when an object or information is created.

Refinement:

The security attributes concerned by these requirements are:

- the security attribute AT.non_operational_context_complete that indicates that all required information are specified for the associated non operational context (OB.timestamping_context with security attribute AT.context_operational being "False"),
- the security attribute AT.non_operational_context_created that indicates that a non operational context (OB.timestamping_context with security attribute AT.context_operational being "False") is created,
- the security attribute AT.context_operational that indicates that the context it is associated with (OB.timestamping_context) is operational,
- the security attribute AT.monotonic_timestamp_token_time associated with a timestamping context (OB.timestamping_context) that indicates if the time value provided by the internal clock for the current timestamp token is greater than the time value placed in the previous timestamp token generated by this timestamping context.

FMT_MSA.1/Context Management of security attributes

FMT_MSA.1.1/Context [Editorial refinement] The TSF shall enforce the **following policies:**

- **context management policy,**
- **key management policy,**
- **timestamp token generation policy,**

to restrict the ability to:

- **modify and query** the security attributes **AT.non_operational_context_complete, AT.non_operational_context_created and AT.context_operational** to **the Security Administrator**,
- **modify** the security attribute **AT.monotonic_timestamp_token_time** to **no role** (this security attribute is directly modified by the TOE).

Refinement:

The modification operation on the following security attributes:

- AT.non_operational_context_complete,
- AT.context_operational,

are performed indirectly by the Security Administrator, since these attribute modifications result from operations performed by the Security Administrator (context creation and certificate import).

The Security Administrator can only specify that a non operational context is created (i.e., the Security Administrator can only modify the security attribute AT.non_operational_context_created from the "False" to the "True" value only).

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.

Refinement:

The security attribute AT.non_operational_context_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 Security Administrator.

FMT_SMF.1/Context Specification of Management Functions

FMT_SMF.1.1/Context The TSF shall be capable of performing the following management functions:

- **modification of the following security attributes:**
  - **AT.non_operational_context_complete,**
  - **AT.non_operational_context_created,**
  - **AT.context_operational,**
  - **AT.monotonic_timestamp_token_time,**
- **querying of the following security attributes:**
  - **AT.non_operational_context_complete,**
  - **AT.non_operational_context_created,**
  - **AT.context_operational**.

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

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

Refinement:

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

- identification of the internal clock 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,
- initial validity period of the context private key,
- reference(s) of accepted timestamping policies,
- identifier(s) of authorized hash algorithms for each timestamping policy.

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

FDP_ITC.1.3/Context 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 Stored data integrity monitoring and action

FDP_SDI.2.1/Context 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]**.

Refinement:

The user data correspond to the timestamping contexts.

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

6.1.2 Key management policy

FDP_ETC.1/Non_Operational_Context_Public_Key Export of user data without security attributes

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

FDP_ETC.1.2/Non_Operational_Context_Public_Key The TSF shall export the user data without the user data's associated security attributes

Refinement:

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

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

Refinement:

The imported user data are the public key certificates of timestamping units delivered by a Certification Authority.

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

FDP_ITC.2.3/Timestamping_Unit_Certificate 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/Timestamping_Unit_Certificate 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/Timestamping_Unit_Certificate The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **rules defined in the key management policy**.

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

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

FPT_TDC.1.2/Timestamping_Unit_Certificate The TSF shall use

- **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,**
- **the value of the private key validity period extension field of the imported certificate, if present, to derive the effective private key validity period for the context private key,** when interpreting the TSF data from another trusted IT product.

FTP_TRP.1/Timestamping_Unit_Certificate Trusted path

FTP_TRP.1.1/Timestamping_Unit_Certificate The TSF shall provide a communication path between itself and **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 **modification and disclosure**.

FTP_TRP.1.2/Timestamping_Unit_Certificate The TSF shall permit **local users** to initiate communication via the trusted path.

FTP_TRP.1.3/Timestamping_Unit_Certificate The TSF shall require the use of the trusted path for **initial user authentication**.

Refinement:

Local users referred to in these requirements are the Security Administrators of the TOE who import timestamping unit certificates into the TOE.

FDP_IFC.1/Key_Management_Policy Subset information flow control

FDP_IFC.1.1/Key_Management_Policy The TSF shall enforce the **key management policy** on**:**

- **Information:**
  - **value of the timestamping unit certificate imported into the TOE (I.imported_certificate),**
  - **value of the public key contained in the timestamping unit certificate imported into the TOE (I.imported_certificate_public_key),**
  - **value of the public key of the non operational context into which the certificate is imported (I.non_operational_context_public_key),**
  - **value of the private key of the non operational context into which the certificate is imported (I.non_operational_context_private_key),**
  - **value of the private key validity period contained in the timestamping unit certificate imported into the TOE, if present (I.imported_certificate_private_key_validity_period),**
  - **value of the public key algorithm identifier (I.public_key_algorithm_identifier),**
- **Subjects: subjects that export the public key generated by the TOE and import the corresponding public key certificate of the timestamping unit into the TOE to create an operational context (S.public_key_export_module and S.timestamping_unit_certificate_import_module respectively),**
- **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.timestamping_context)**.

FDP_IFF.1/Key_Management_Policy Simple security attributes

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

- **the security attributes AT.non_operational_context_complete and AT.non_operational_context_created associated with a non operational context (OB.timestamping_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 Administrator,**
- **the security attribute AT.context_operational that indicates that a timestamping context (OB.timestamping_context) is operational following the authorized import of the timestamping unit certificate,**
- **the security attributes AT.private_key_initial_validity_period associated with a non operational context (OB.timestamping_context with security attribute AT.context_operational being "False") and AT.private_key_effective_validity_period associated with an operational context (OB.timestamping_context with security attribute AT.context_operational being "True") that concern the validity period of the private key of the timestamping context,**
- **[assignment: other security attributes]**.

Refinement:

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

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

- **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 (I.non_operational_context_public_key and I.public_key_algorithm_identifier) from the non operational context (OB.timestamping_context with security attribute being "False") by the subject that exports the public key (S.public_key_export_module). This operation is authorized to be performed only on behalf of an authenticated Security Administrator,**
- **the operation OP.timestamping_unit_certificate_import enables the import of the certificate corresponding to the exported public key (I.timestamping_unit_certificate) into the non operational context (OB.timestamping_context with security attribute AT.context_operational being "False") by the subject that imports the certificate (S.timestamping_unit_certificate_import_module) in order to create the corresponding operational context (OB.timestamping_context with security attribute AT.context_operational being "True"). This operation is authorized to be performed only on behalf of an authenticated Security Administrator only if the following conditions hold:**

- **the non operational context is both complete and created (the value of the security attributes AT.non_operational_context_complete and AT.non_operational_context_created are both "True"),**
- **the value of the public key of the imported certificate (I.imported_certificate_public_key) corresponds to the value of the public key of the non operational context into which the timestamping certificate is imported (I.non_operational_context_public_key)**.

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

FDP_IFF.1.4/Key_Management_Policy The TSF shall explicitly authorise an information flow based on the following rules:

- **derivation of the effective private key validity period (AT.private_key_effective_validity_period) associated with the private key of a non operational context. The derivation is based on the following rules:**
  - **If the imported certificate contains a private key validity period extension field, the value of the private key validity period defined during the context creation phase (AT.private_key_initial_validity_period) by an authenticated Security Administrator is ignored and the value contained in the imported certificate is considered as the effective private key validity period.**
  - **If the imported certificate does not contain a private key validity period extension field, the value of the private key validity period defined during the context creation phase by an authenticated Security Administrator is considered as the effective private key validity period.**
- **destruction of the private key of a non operational context if the associated private key validity period specified during the context creation phase (AT.private_key_initial_validity_period) has expired.**
- **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/Key_Management_Policy The TSF shall explicitly deny an information flow based on the following rules:

- **private keys (I.non_operational_context_private_key) generated by the TOE shall never be exported outside the TOE,**
- **private keys (I.non_operational_context_private_key) and key pairs (I.non_operational_context_private_key and I.non_operational_context_public_key) generated outside the TOE shall never be imported into the TOE,**
- **timestamping certificates (I.imported_certificate) shall not be imported into an operational context (OB.timestamping_context with security attribute AT.context_operational being "True")**.

Refinement:

The TOE shall provide a means for:

- deducing the right validity period for the private key (AT.private_key_effective_validity_period) associated with the private key of a non operational context.
- destroying the private key of a non operational context if the associated private key that has been created during the context creation phase (AT.private_key_initial_validity_period) has expired.
- destroying the private key of an operational context if the associated effective private key validity period (AT.private_key_effective_validity_period) has expired

FMT_MSA.3/Private_Key_Validity_Period Static attribute initialisation

FMT_MSA.3.1/Private_Key_Validity_Period The TSF shall enforce the **following policies:**

- **key management policy,**
- **timestamp token generation policy,** to provide **the private key initial validity period specified by the Security Administrator during the context creation phase and the private key effective validity period computed by the TOE during the timestamping certificate import as** default values for security attributes that are used to enforce the SFP.

Refinement:

The derivation of the effective private key validity period by the TOE (AT.private_key_effective_validity_period) is based on the following rule:

- If the imported certificate contains a private key validity period extension field, the value of the private key validity period defined during the context creation phase (AT.private_key_initial_validity_period) by an authenticated Security Administrator is ignored and the value contained in the imported certificate is considered as the effective private key validity period.
- If the imported certificate does not contain a private key validity period extension field, the value of the private key validity period defined during the context creation phase by an authenticated Security Administrator is considered as the effective private key validity period.

FMT_MSA.3.2/Private_Key_Validity_Period The TSF shall allow the **following role: none** to specify alternative initial values to override the default values when an object or information is created.

Refinement:

The security attributes concerned by these requirements are AT.private_key_initial_validity_period and AT.private_key_effective_validity_period.

FMT_MSA.1/Private_Key_Validity_Period Management of security attributes

FMT_MSA.1.1/Private_Key_Validity_Period [Editorial refinement] The TSF shall enforce the **following policies:**

- **key management policy,**
- **timestamp token generation policy,**

to restrict the ability to:

- **query** the security attribute **AT.private_key_initial_validity_period** and
- **query and modify** the security attribute **AT.private_key_effective_validity_period**

to **the Security Administrator**.

Refinement:

The modification operation on the security attribute AT.private_key_effective_validity_period is performed indirectly by the Security Administrator, since this attribute modification results from an operation performed by the Security Administrator (certificate import).

FMT_SMF.1/Private_Key_Validity_Period Specification of Management Functions

FMT_SMF.1.1/Private_Key_Validity_Period The TSF shall be capable of performing the following management functions:

- **modification of the security attribute AT.private_key_effective_validity_period,**
- **querying of the security attributes AT.private_key_initial_validity_period and AT.private_key_effective_validity_period**.

FCS_CKM.1/Context_Keys Cryptographic key generation

FCS_CKM.1.1/Context_Keys 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: **[CRYPTO-STD], [assignment: list of standards]**.

Refinement:

This requirement concerns the asymmetric key pairs used to create and verify the signature of timestamping tokens generated by a timestamping unit.

Application note

The reference document defined by DCSSI [KEYS_STD] for cryptographic key management must be followed.

FCS_CKM.4/Context_Keys Cryptographic key destruction

FCS_CKM.4.1/Context_Keys 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]**.

Refinement:

This requirement concerns private keys contained in both operational and non operational contexts.

Application note

The reference document defined by DCSSI [KEYS_STD] for cryptographic key management must be followed.

FMT_MSA.2/Context_Keys Secure security attributes

FMT_MSA.2.1/Context_Keys The TSF shall ensure that only secure values are accepted for **the private key validity period (AT.private_key_effective_validity_period).**.

6.1.3 Policy of time-stamp tokens generation

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

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

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

FDP_ITC.1.3/Timestamp_Token_Request The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **rules defined in the timestamp token generation policy**.

FDP_ETC.1/Timestamp_Token Export of user data without security attributes

FDP_ETC.1.1/Timestamp_Token The TSF shall enforce the **timestamp token generation policy** when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.1.2/Timestamp_Token The TSF shall export the user data without the user data's associated security attributes

Refinement:

The exported user data are the timestamp tokens delivered by the timestamping system.

FDP_IFC.1/Timestamp_Token_Generation_Policy Subset information flow control

FDP_IFC.1.1/Timestamp_Token_Generation_Policy The TSF shall enforce the **timestamp token generation policy** on**:**

- **Information:**
  - **value of the imported timestamp token request (I.timestamp_token_request),**
  - **value of the hash algorithm identifier used to generate the data imprint contained in the imported timestamp token request (I.hash_algorithm_identifier),**
  - **value of the data imprint contained in the imported timestamp token request (I.data_imprint),**
  - **value of the timestamping policy identifier contained in the imported timestamp token request, if present (I.request_policy_identifier),**
  - **value of the nonce contained in the imported timestamp token request, if present (I.request_nonce),**
  - **value of the time contained in the exported timestamp token (I.timestamp_token_time),**
  - **value of the timestamping unit certificate reference (I.timestamping_unit_certificate_reference)**
  - **value of the used timestamping policy contained in the exported timestamp token (I.used_timestamping_policy_identifier),**
  - **value of the timestamp token signature (I.timestamp_token_signature).**
- **Subjects: subjects that import timestamp token requests and exports signed timestamp tokens as responses to such requests (S.timestamp_token_request_import_module and S.timestamp_token_export_module respectively).**
- **Operations: import of timestamp token requests (OP.timestamp_token_request_import), and export of signed timestamp tokens (OP.timestamp_token_export).**
- **Objects: timestamp tokens (OB.timestamp_token)**.

FDP_IFF.1/Timestamp_Token_Generation_Policy Simple security attributes

FDP_IFF.1.1/Timestamp_Token_Generation_Policy The TSF shall enforce the **timestamp token generation policy** based on the following types of subject and information security attributes:

- **the security attribute AT.context_operational associated with a timestamping context (OB.timestamping_context) that indicates that timestamp tokens can be generated using the information specified in this context,**
- **the security attribute AT.internal_clock_synchronized associated with a timestamping context (OB.timestamping_context) 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 by an authenticated Security Administrator,**
- **[assignment: other security attributes]**.

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

- **the operation OP.timestamp_token_request_import enables the import of timestamp token requests (I.timestamp_token_request) by the subject that import timestamp token requests (S.timestamp_token_request_import_module). This operation is only authorized if the following conditions hold:**
  - **the value of the timestamping policy identifier contained in the request, if present (I.request_policy_identifier) references a timestamping policy accepted by the timestamping system (i.e., there exists at least one timestamping context whose security attribute AT.context_operational is "True" that accepts this policy) and a default timestamping policy has been defined by an authenticated Security Administrator to be used in the case a timestamping policy identifier is not specified in the request (the security attribute AT.default_timestamping_policy_defined is "True"),**
  - **the value of the hash algorithm identifier contained in the request (I.hash_algorithm_identifier) is authorized by the used timestamping policy defined in the used operational context (OB.timestamping_context with security attribute AT.context_operational being "True"),**
  - **the length of the data imprint contained in the request (I.data_imprint) is consistent with the hash algorithm identifier (I.hash_algorithm_identifier),**
  - **the internal clock referenced in the used operational context is synchronized with UTC with the accuracy defined in the used operational context (the security attribute AT.internal_clock_synchronized is "True"),**

- **the operation OP.timestamp_token_export enables the export of signed timestamp tokens that contain all information present in the corresponding requests (I.timestamp_token_request), the value of the timestamping unit certificate reference (I.timestamping_unit_certificate_reference), the value of the used timestamping policy (I.used_timepstamping_policy_identifier), the value of the time provided by the used internal clock (I.timestamp_token_time), the value of the nonce if present in the token request (I.request_nonce) and the value of the timestamp token signature (I.timestamp_token_signature) by the subject that export timestamp tokens (S.timestamp_token_export_module). This operation is only authorized if the following conditions hold:**
  - **the internal clock referenced in the used operational context is synchronized with UTC with the accuracy defined in the used operational context (the security attribute AT.internal_clock_synchronized is "True")**.

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

FDP_IFF.1.4/Timestamp_Token_Generation_Policy The TSF shall explicitly authorise an information flow based on the following rules: **timestamp token requests that conform to the expected request format shall be imported into the TOE**.

FDP_IFF.1.5/Timestamp_Token_Generation_Policy The TSF shall explicitly deny an information flow based on the following rules: **timestamp token requests that do not conform to the expected request format shall not be imported into the TOE**.

Refinement:

The ST author shall specify the expected timestamp request format.

FMT_MSA.3/Default_Timestamping_Policy Static attribute initialisation

FMT_MSA.3.1/Default_Timestamping_Policy The TSF shall enforce the **timestamp token generation policy** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/Default_Timestamping_Policy The TSF shall allow the **Security Administrator** to specify alternative initial values to override the default values when an object or information is created.

Refinement:

These requirements concern the security attribute AT.default_timestamping_policy_defined. The Security Administrator can specify an alternative value for this security attribute by specifying the reference of the default timestamping policy for the timestamping system.

FMT_MSA.3 / Internal_Clock Static attribute initialisation

FMT_MSA.3.1 / Internal_Clock The TSF shall enforce the **timestamp token generation policy** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 / Internal_Clock The TSF shall allow the **Security Administrator** to specify alternative initial values to override the default values when an object or information is created.

Refinement:

These requirements concern the security attribute AT.internal_clock_synchronized. The Security Administrator can specify an alternative value for this security attribute at the time of the initial synchronization of the internal clock during the timestamping unit initialization phase.

FMT_MSA.1 / Default_Timestamping_Policy Management of security attributes

FMT_MSA.1.1 / Default_Timestamping_Policy The TSF shall enforce the **timestamp token generation policy** to restrict the ability to **modify and query** the security attributes **AT.default_timestamping_policy_defined** to **the Security Administrator**.

FMT_MSA.1 / Internal_Clock Management of security attributes

FMT_MSA.1.1 / Internal_Clock The TSF shall enforce the **timestamp token generation policy** to restrict the ability to **query and modify** the security attributes **AT.internal_clock_synchronized** to **the Security Administrator (and the TOE for the modification operation)**.

FDP_ACC.1 / Timestamp_Token_Generation_Policy Subset access control

FDP_ACC.1.1 / Timestamp_Token_Generation_Policy The TSF shall enforce the **timestamp token generation policy** on

- **Objects: operational contexts (OB.timestamping_context with security attribute AT.context_operational being "True") generating timestamp tokens signed against the context signature private key, and generated timestamp tokens (OB.timestamp_token) containing the information present in the corresponding timestamp token requests (I.timestamp_token_request), the time value provided by the used internal clock (I.timestamp_token_time), the value of the timestamping unit certificate reference (I.timestamping_unit_certificate_reference) and the value of the used timestamping policy (I.used_timestamping_policy_identifier),**

- **Subjects: subject that generates signed timestamp tokens (S.timestamp_token_generation_module),**
- **Operations: creation and signature of timestamp tokens (OP.timestamp_token_creation and OP.timestamp_token_signature respectively)**.

FDP_ACF.1/Timestamp_Token_Generation_Policy Security attribute based access control

FDP_ACF.1.1/Timestamp_Token_Generation_Policy The TSF shall enforce the **timestamp token generation policy** to objects based on the following:

- **the security attribute AT.context_operational that indicates if the timestamping context (OB.timestamping_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.timestamping_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.internal_clock_synchronized associated with the used operational context (OB.timestamping_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 Administrator,**
- **[assignment: other security attributes]**.

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

- **the creation of timestamp tokens (OP.timestamp_token_creation on OB.timestamp_token) is authorized to be performed only by the subject that generates timestamp tokens (S.timestamp_token_generation_module) only 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.timestamping_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_defined is "True"),**
- **the used internal clock is synchronized with UTC with the accuracy defined in the used operational context (the security attribute AT.internal_clock_synchronized is "True"),**

o **the signature of timestamp tokens (OP.timestamp_token_signature on OB.timestamp_token) is authorized to be performed by the subject that generates timestamp tokens (S.timestamp_token_generation_module) only 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.timestamping_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.internal_clock_synchronized is "True")**.

FDP_ACF.1.3 / Timestamp_Token_Generation_Policy The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

o **if all the rules stated in FDP_ACF.1.2 are satisfied**.

FDP_ACF.1.4 / Timestamp_Token_Generation_Policy The TSF shall explicitly deny access of subjects to objects based on the

o **if one of the rules stated in FDP_ACF.1.2 is not satisfied**.

FCS_COP.1 / Timestamp_Token Cryptographic operation

FCS_COP.1.1 / Timestamp_Token The TSF shall perform **asymmetric signature generation** in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithm]** and cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **[CRYPTO-STD], [assignment: list of standards]**.

Refinement:

This operation is used to generate digital signatures on the timestamp tokens delivered by the TOE.

Application note

If the signature algorithm is a signature algorithm with appendix, the algorithm comprises an asymmetric signature algorithm and a hashing function.

Moreover, the reference document defined by DCSSI [KEYS_STD] for cryptographic key management must be followed.

FMT_SMF.1/Default_Timestamping_Policy Specification of Management Functions

FMT_SMF.1.1/Default_Timestamping_Policy The TSF shall be capable of performing the following management functions:

- **Definition by an authenticated Security Administrator using a timestamping policy identifier of the default timestamping policy to be applied by the timestamping system when no timestamping policy is specified in the timestamp token request,**
- **Definition by an authenticated Security Administrator using hash algorithm identifiers of the authorized hash algorithms accepted for the default timestamping policy,**
- **Modification and querying of the security attribute AT.default_timestamping_policy_defined**.

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

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

Refinement:

The imported user data correspond to the reference of the default timestamping policy defined by the Security Administrator.

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

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

FMT_SMF.1 / Internal_Clock Specification of Management Functions

FMT_SMF.1.1 / Internal_Clock The TSF shall be capable of performing the following management functions:

- **query the security attribute AT.internal_clock_synchronized,**
- **set the security attribute AT.internal_clock_synchronized to "Synchronized" if the internal clock is synchronized with UTC with the accuracy defined in the used operational context (function identified by OP.set_to_synchronized),**
- **set the security attribute AT.internal_clock_synchronized to "Not synchronized" if the internal clock is not synchronized with UTC with the accuracy defined in the used operational context (function identified by OP.set_to_not_synchronized),**
- **synchronize the internal clock of a timestamping unit (function identified by OP.synchronize),**
- **periodically compare the time difference between the internal clock of a timestamping unit and the time reference with an authorized value: if the time difference is greater than the authorized value then OP.set_to_not_synchronized is performed, otherwise OP.set_to_synchronized is performed,**
- **periodically record the time difference between the internal clock of a timestamping unit and the time reference to create and update an history of those time gap,**
- **periodically verify the synchronization of the internal clock of a timestamping unit by making use of the history of time difference between this internal clock and the time reference: if the history of the time difference is not in conformance with the drift authorized over a given time period then OP.set_to_not_synchronized is performed, otherwise OP.synchronize is performed depending on the decision made by the synchronization verification algorithm,**
- **initialize the time reference and the internal clock during the initialization phase of a timestamping unit,**
- **update the time reference: this function shall be performed right before the periodic comparison since the time reference represents a local approximation of UTC time**.

FMT_MTD.1 / Internal_Clock Management of TSF data

FMT_MTD.1.1 / Internal_Clock The TSF shall restrict the ability to **initialize** the **internal clock of a timestamping unit** to **the Security Administrator**.

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

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

Refinement:

The imported user data correspond to the time value used to synchronize the internal clock during the initialization phase of a timestamping unit and the information required to initialize and update the time reference.

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

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

FMT_SMF.1/Temporary_Interruption Specification of Management Functions

FMT_SMF.1.1/Temporary_Interruption The TSF shall be capable of performing the following management functions:

- **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.internal_clock_synchronized is "False")**.

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

FPT_TDC.1.1/Hash_Algorithms The TSF shall provide the capability to consistently interpret **the cryptographic hash algorithm identifiers associated with each accepted timestamping policy** when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/Hash_Algorithms The TSF shall use **[assignment: list of interpretation rules to be applied by the TSF]** when interpreting the TSF data from another trusted IT product.

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

FPT_TDC.1.1/Timestamping_Policies The TSF shall provide the capability to consistently interpret **the timestamping policy identifiers that can be contained in timestamping token requests** when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/Timestamping_Policies The TSF shall use **[assignment: list of interpretation rules to be applied by the TSF]** when interpreting the TSF data from another trusted IT product.

6.1.4 Physical Attacks

FPT_PHP.1 Passive detection of physical attack

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

FPT_PHP.3 Resistance to physical attack

FPT_PHP.3.1 The TSF shall resist **[assignment: physical tampering scenarios]** to the **[assignment: list of TSF devices/elements]** by responding automatically such that the SFRs are always enforced.

Refinement:

The TOE shall destroy the private keys of the different timestamping contexts when physical attacks are detected.

6.1.5 Rôles

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles

- **Security Administrator,**
- **Auditor**.

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

FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.2 User authentication before any action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Refinement:

The users referred to in this requirement are the Administrators (Security administrator and Auditor) of the TOE.

6.1.6 TSF protection

FPT_TST.1 TSF testing

FPT_TST.1.1 The TSF shall run a suite of self tests **at the conditions of a return to an operational state following a temporary service interruption, [assignment: other conditions under which self test should occur], at the request of the authorised user and during initial start-up** to demonstrate the correct operation of **the TSF**.

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of **TSF data**.

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

Refinement:

The authorized user referred to in these requirements is the Security Administrator of the TOE.

FPT_RCV.2 Automated recovery

FPT_RCV.2.1 When automated recovery from**:**

- **loss of synchronization for internal clocks (i.e., the security attribute AT.internal_clock_synchronized is "False"),**
- **[assignment: list of other failures/service discontinuities]** is not possible, the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.

Refinement:

Return to a secure state when automated recovery is not possible is authorized only to be performed by a Security Administrator.

FPT_RCV.2.2 For **[assignment: list of failures/service discontinuities]**, the TSF shall ensure the return of the TOE to a secure state using automated procedures.

6.1.7 Audit and security alarms

FAU_GEN.1/Internal_Clock Audit data generation

FAU_GEN.1.1/Internal_Clock 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 **detailed** level of audit; and

c) **for each internal clock:**

- **last successful comparison between the internal clock and the time reference (date of comparison operation and values of internal clock and time reference),**
- **synchronizations of the internal clock (date of synchronization operation and value of synchronization correction),**
- **[assignment: other specifically defined auditable events]**.

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

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) 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]**.

Refinement:

The audit events considered in these requirements concern the verifications of synchronization and the synchronizations of the timestamping unit internal clocks.

FAU_GEN.1/Administration Audit data generation

FAU_GEN.1.1/Administration 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 **detailed** level of audit; and

c) **[assignment: other specifically defined auditable events]**.

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

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) 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]**.

Refinement:

The audit events considered in these requirements concern all operations related to the administration of the TOE.

FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide **Auditors** 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

FAU_SAR.3.1 The TSF shall provide the ability to apply **searches, sorting and/or ordering** of audit data based on **[assignment: criteria with logical relations]**.

FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to **prevent** unauthorised modifications to the stored audit records in the audit trail.

FAU_ARP.1/Security_Alarm Security alarms

FAU_ARP.1.1/Security_Alarm The TSF shall take **the following actions:**

- **a security alarm is raised to the Security Administrator and to the Auditor,**
- **[assignment: list of the other least disruptive actions]** upon detection of a potential security violation.

Refinement:

The ST author can specify other least disruptive actions by completing the assignment.

FAU_SAA.1/Security_Alarm Potential violation analysis

FAU_SAA.1.1/Security_Alarm The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2/Security_Alarm The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of**:**

- **repeat synchronizations of the internal clock of a timestamping unit,**
- **[assignment: subset of defined auditable events]** known to indicate a potential security violation;

b) **other rules:**

- **memory used to store audit events close to its maximum storage capacity,**
- **instantaneous time difference between the internal clock of a timestamping unit and the time reference greater than an authorized value,**
- **history of the time difference between the internal clock of a timestamping unit and the time reference not in conformance with the drift authorized over a given period of time,**
- **[assignment: any other rules]**.

FPT_STM.1 Reliable time stamps

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

Refinement:

Those reliable time stamps are provided by the TSF for its own use.

FAU_STG.4 Prevention of audit data loss

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.

FAU_STG.2 Guarantees of audit data availability

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 **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]**

6.2 Security assurance requirements

The required level of security assurance is EAL3 augmented with AVA_VAN.3 and ALC_FLR.3.

7 Rationales

7.1 Security objectives rationale

7.1.1 Threats coverage

7.1.1.1 Threats on time-stamping context

T.CONTEXT_MODIFICATION This threat is countered by O.NON_OPERATIONAL_CONTEXT_CREATION which guarantees that the value of the key pair of a non operational time-stamping context cannot be modified and that other information of a non operational context can be modified only by the Security administrator as long as the non operational time-stamping context is not declared as created. Moreover, information of a non operational time-stamping context declared as created is not modifiable individually and can be only completely deleted by the Security administrator.

O.OPERATIONAL_CONTEXT_PROTECTION ensures in addition that information present in an operational context is not modifiable.

Moreover, O.ADMIN_AUTHENTICATION allows ensuring that only the authenticated security administrators can create time-stamping contexts.

O.ADMINISTRATION_LOGS and O.ALARMS cover all the threats on the sensitive assets of the TOE, because they ensure that the operations realized on these sensitive assets are traced and that security alarms are generated to report malfunctions of the TOE whether having an accidental or a malicious nature. They thus allow to detect and to treat errors or attacks after analysis of the audit events and security alarms.

7.1.1.2 Threats on time-stamp unit internal clock

T.CLOCK_MODIFICATION This threat is countered by O.CONTEXT_STOPS which ensures the destruction of the time-stamping context in the event of attacks detection on the time-stamping unit. Moreover, O.ADMIN_AUTHENTICATION allows to ensure that only the authenticated security administrators can realize the initial synchronization of the clock included in the creation phase of a time-stamping context.

OE.TIME_REFERENCE guarantees that the TOE can detect a gap between the time-stamping unit internal clock and the time reference because it ensures that no attack can compromise simultaneously and in a coherent way these two values.

O.TIMESTAMPING_UNIT_LOGS guarantees that all the operations of comparison between the values of the time-stamping unit internal clock and of the time reference and the operations synchronization of the internal clock will be traced to be consulted by the Auditor.

O.ADMINISTRATION_LOGS and O.ALARMS cover all the threats on the sensitive assets of the TOE, because they ensure that the operations realized on these sensitive assets are traced and that security alarms are generated to report malfunctions of the TOE whether having an accidental or a malicious nature. They thus allow to detect and to treat errors or attacks after analysis of the audit events and security alarms.

T.TIME_GAP_HISTORY_MODIFICATION This threat is countered by:

O.SECURE_STATE_RETURN covers the threats which modify or disclose the sensitive assets of the TOE in a way not authorized, because it guarantees that the TOE is always in a secure state.

O.ADMINISTRATION_LOGS and O.ALARMS cover all the threats on the sensitive assets of the TOE, because they ensure that the operations carried out on these assets are traced and that security alarms are generated to report malfunctions of the TOE whether having an accidental or a malicious nature.

7.1.1.3 Threats on time-stamp token requests

T.REQUEST_FORGERY This threat is countered by O.REQUEST_VERIFICATION which guarantees that the conformance of the format of the time-stamp token request received with respect to the awaited format is checked by the TOE. Moreover, O.HASH_VERIFICATION specifically covers the checking of the digest length of document with respect to the referred hash algorithm.

T.INCOHERENT_HASH This threat is countered by O.HASH_VERIFICATION which guarantees coherence between the digest length of document present in the time-stamp token request and the referred hash algorithm. O.HASH_VERIFICATION also ensures that the referred hash algorithm is authorized by the applied time-stamp policy. Moreover, O.REQUEST_VERIFICATION guarantees the overall coherence of the request received with respect to the awaited format.

7.1.1.4 Threats on cryptographic keys

T.KEYS_DISCLOSURE This threat is countered by O.KEYS_IMPORT and O.KEYS_EXPORT which guarantee that only the private keys generated by the TOE can be used to sign the time-stamp tokens, and that these private keys cannot be exported outside of the TOE. O.CONTEXT_STOPS ensures that the various time-stamping contexts will be stopped and that the private keys of these contexts will be destroyed in the event of attacks detection.

O.CRYPTO guarantees a correct cryptographic keys management on the TOE, including the key pairs generation and of the private keys destruction. Moreover, O.ADMIN_AUTHENTICATION allows ensuring that only the authenticated security administrators can realize the key pairs generation on the TOE.

O.ADMINISTRATION_LOGS and O.ALARMS cover all the threats on the sensitive assets of the TOE, because they ensure that the operations carried out on these sensitive assets are traced and that security alarms are generated to report malfunctions of the TOE whether having an accidental or a malicious nature. They thus allow to detect and to treat errors or attacks after analysis of the audit events and security alarms.

T.ADMIN_AUTH_DATA_DISCLOSURE This threat is countered by OE.ADMIN which ensures that the administrators of the TOE are correctly trained for the tasks which they have to realize on the TOE and who require their identification and their authentication. Moreover, OE.TIMESTAMPING_ AUTHORITY guarantees that the administrators observe the rules of the time-stamp policies supported by the Time-stamping authority.

OE.LOCAL_ADMIN guarantees that the administration of the TOE can be carried out only locally from a secure environment with controlled access.

O.ADMINISTRATION_LOGS and O.ALARMS cover all the threats on the sensitive assets of the TOE, because they ensure that the operations carried out on these sensitive assets are traced and that security alarms are generated to report malfunctions of the TOE whether having an accidental or a malicious nature. They thus allow to detect and to treat errors or attacks after analysis of the audit events and security alarms.

T.ADMIN_AUTH_DATA_MODIFICATION This threat is countered by OE.ADMIN which ensures that the administrators of the TOE are correctly trained for the tasks which they have to realize on the TOE and who require their identification and their authentication. Moreover, OE.TIMESTAMPING_ AUTHORITY guarantees that the administrators observe the rules of the time-stamp policies supported by the Time-stamping authority.

OE.LOCAL_ADMIN guarantees that the administration of the TOE can be carried out only locally from a secure environment with controlled access.

O.ADMINISTRATION_LOGS and O.ALARMS cover all the threats on the sensitive assets of the TOE, because they ensure that the operations carried out on these sensitive assets are traced and that security alarms are generated to report malfunctions of the TOE whether having an accidental or a malicious nature. They thus allow to detect and to treat errors or attacks after analysis of the audit events and security alarms.

7.1.1.5 Threats on time-stamping unit state

T.POWER_STATE_MODIFICATION This threat is countered by O.INTERRUPTION which guarantees that the services of time-stamp tokens generation will be stopped in the event of power failure.

O.SECURE_STATE_RETURN covers the threats which modify or disclose the sensitive assets of the TOE in a way not authorized, because it guarantees that the TOE is always in a secure state.

O.ADMINISTRATION_LOGS and O.ALARMS cover all the threats on the sensitive assets of the TOE, because they ensure that the operations carried out on these sensitive assets are traced and that security alarms are generated to report malfunctions of the TOE whether having an accidental or a malicious nature.

T.SYNCHRO_STATE_MODIFICATION This threat is countered by O.INTERRUPTION which guarantees that the services of time-stamp tokens generation will be stopped when the state of synchronization of the internal clock does not allow guaranteeing the accuracy required by the applied time-stamp policy.

O.SECURE_STATE_RETURN covers the threats which modify or disclose the sensitive assets of the TOE in a way not authorized, because it guarantees that the TOE is always in a secure state.

O.ADMINISTRATION_LOGS and O.ALARMS cover all the threats on the sensitive assets of the TOE, because they ensure that the operations carried out on these sensitive assets are traced and that security alarms are generated to report malfunctions of the TOE whether having an accidental or a malicious nature.

7.1.1.6 Threats on administration

T.ADMIN_USURPATION This threat is countered by O.ADMIN_AUTHENTICATION because this objective imposes the authentication of the administrators before being able to perform operations of administration on the TOE.

O.ADMINISTRATION_LOGS and O.ALARMS cover all the threats on the sensitive assets of the TOE, because they ensure that the operations carried out on these sensitive assets are traced and that security alarms are generated to report malfunctions of the TOE whether having an accidental or a malicious nature. They thus allow to detect and to treat errors or attacks after analysis of the audit events and security alarms.

7.1.1.7 Threats on audit

T.AUDIT_RECORDS_MODIFICATION This threat is countered by O.AUDIT_RECORDS_PROTECTION and O.ADMIN_AUTHENTICATION which guarantee the integrity of the audit events and impose that the recordings of audit events can be removed only by auditors authenticated as such.

O.ADMINISTRATION_LOGS and O.ALARMS cover all the threats on the sensitive assets of the TOE, because they ensure that the operations carried out on these sensitive assets are traced and that security alarms are generated to report malfunctions of the TOE whether having an accidental or a malicious nature. They thus allow to detect and to treat errors or attacks after analysis of the audit events and security alarms.

7.1.2 OSP coverage

OSP.SERVICES This OSP is covered by O.TOKEN_GENERATION, O.INTERNAL_CLOCK and O.INTERRUPTION which guarantee that the TOE provides the services of time-stamp tokens generation containing a time whose accuracy with UTC time is guaranteed.

O.CRYPTO also covers this OSP because it guarantees a correct keys management during the signature of the time-stamp tokens.

OSP.CRYPTO This OSP is covered by O.CRYPTO for the implementation of the cryptographic functions and cryptographic key management and authentication data. It is also covered by:

- O.ADMIN_AUTHENTICATION for the authentication of the administrators,
- O.TOKEN_GENERATION for the time-stamp token generation.

OSP.INTERNAL_CLOCK_SYNCHRONIZATION This OSP is covered by O.INTERNAL_CLOCK which guarantees that the time-stamping unit internal clock is maintained synchronized with UTC. Moreover, O.ADMIN_AUTHENTICATION allows ensuring that only the authenticated security administrators can carry out the initial synchronization of the clock included in the creation phase of a time-stamping context.

O.ADMINISTRATION_LOGS and O.ALARMS also cover this OSP, because they ensure that the operations carried out on these sensitive assets are traced and that security alarms are generated to report malfunctions of the TOE whether having an accidental or a malicious nature. They thus allow to detect and to treat errors or attacks after analysis of the audit events and security alarms. Moreover, O.TIMESTAMPING_UNIT_LOGS guarantees that all the operations of comparison between the values of the time-stamping

unit internal clock and of the time reference and the operations synchronization of the internal clock will be traced to be consulted by the Auditor.

OSP.DEFAULT_POLICY This OSP is covered by O.DEFAULT_POLICY.

OSP.CONTEXT_MANAGEMENT This OSP is covered by O.NON_OPERATIONAL_CONTEXT_CREATION which guarantees that non operational time-stamping contexts can be created by a Security administrator, by O.CONTEXTS_VISUALIZATION which ensures that the contained information in the time-stamping contexts (except for the private key of the context) are consultable by a Security administrator, and by O.CONTEXT_STOP which guarantees that the time-stamping contexts can be definitively stopped.

OSP.CERTIFICATE_IMPORTATION This OSP is covered by O.CERTIFICATE_IMPORTATION.

OSP.REQUEST_PROTOCOL This OSP is covered by O.REQUEST_PROTOCOL.

7.1.3 Assumptions coverage

7.1.3.1 Assumptions on the TOE usage

A.TOKEN_VERIFICATION This assumption is supported by OE.TOKEN_VERIFICATION.

A.ADMIN This assumption is supported by OE.ADMIN which imposes the training of the administrators for the tasks for which they have the responsibility.

A.AUDIT This assumption is supported by OE.ANALYZE_AUDIT which imposes the regular analysis of the audit records by the auditor.

7.1.3.2 Assumptions on the TOE operational environment

A.CERTIFICATION_AUTHORITY This assumption is supported by OE.CERTIFICATION_AUTHORITY. OE.CERTIFICATE_IMPORT also supports this assumption because it forces to check, at the time of the time-stamping unit certificate importation, that this one comes well from a Certification Authority entitled to deliver certificates for a given context.

A.TIME_STAMPING_AUTHORITY This assumption is supported by OE.TIMESTAMPING_AUTHORITY. OE.CERTIFICATE_REQUEST also supports this assumption because it imposes the checking of included information in the non operational context at the time of the request for certificate to a Certification Authority.

A.TIME_REFERENCE This assumption is supported by OE.TIME_REFERENCE.

A.LOCATION This assumption is supported by OE.PHYSICAL_PROTECTION and OE.NETWORK which impose that the equipments constituting the TOE are located in a

protected place and is connected on a network which guarantees that the services and the sensitive assets of the TOE will not be compromised.

A.LOCAL_ADMIN This assumption is supported by OE.LOCAL_ADMIN which imposes that the administration of the TOE is performed locally from the secure environment where the TOE is located.

A.NETWORK This assumption is supported by OE.NETWORK which imposes that the equipment constituting the TOE is connected on a network which guarantees that the services and the sensitive assets of the TOE will not be compromised.

A.SUPERVISION This assumption is supported by OE.SUPERVISION which ensures that the operational state of the time-stamping unit can be consulted remotely by a supervisor.

7.1.4 Cover table between problem definition and security objectives

Threats	Security objectives	Rationale
T.CONTEXT_MODIFICATION	O.ADMIN_AUTHENTICATION, O.ADMINISTRATION_LOGS, O.OPERATIONAL_CONTEXT_PROTECTION, O.ALARMS, O.NON_OPERATIONAL_CONTEXT_CREATION	Section 7.1.1
T.CLOCK_MODIFICATION	O.CONTEXT_STOP, O.TIMESTAMPING_UNIT_LOGS, O.ADMIN_AUTHENTICATION, O.ADMINISTRATION_LOGS, O.ALARMS, OE.TIME_REFERENCE	Section 7.1.1
T.TIME_GAP_HISTORY_MODIFICATION	O.SECURE_STATE_RETURN, O.ADMINISTRATION_LOGS, O.ALARMS	Section 7.1.1
T.REQUEST_FORGERY	O.REQUEST_VERIFICATION, O.HASH_VERIFICATION	Section 7.1.1
T.INCOHERENT_HASH	O.REQUEST_VERIFICATION, O.HASH_VERIFICATION	Section 7.1.1
T.KEYS_DISCLOSURE	O.KEYS_EXPORT, O.KEYS_IMPORT, O.ALARMS, O.CONTEXT_STOP, O.CRYPTO, O.ADMIN_AUTHENTICATION, O.ADMINISTRATION_LOGS	Section 7.1.1
T.ADMIN_AUTH_DATA_DISCLOSURE	OE.ADMIN, O.ADMINISTRATION_LOGS, O.ALARMS, OE.TIMESTAMPING_AUTHORITY, OE.LOCAL_ADMIN	Section 7.1.1
T.ADMIN_AUTH_DATA_MODIFICATION	OE.ADMIN, O.ADMINISTRATION_LOGS, O.ALARMS, OE.TIMESTAMPING_AUTHORITY, OE.LOCAL_ADMIN	Section 7.1.1

Threats	Security objectives	Rationale
T.POWER_STATE_MODIFICATION	O.ADMINISTRATION_LOGS, O.ALARMS, O.INTERRUPTION, O.SECURE_STATE_RETURN	Section 7.1.1
T.SYNCHRO_STATE_MODIFICATION	O.ADMINISTRATION_LOGS, O.ALARMS, O.INTERRUPTION, O.SECURE_STATE_RETURN	Section 7.1.1
T.ADMIN_USURPATION	O.ADMINISTRATION_LOGS, O.ALARMS, O.ADMIN_AUTHENTICATION	Section 7.1.1
T.AUDIT_RECORDS_MODIFICATION	O.AUDIT_RECORDS_PROTECTION, O.ALARMS, O.ADMINISTRATION_LOGS, O.ADMIN_AUTHENTICATION	Section 7.1.1

Table 1 Threats coverage by security objectives

Security objectives	Threats
O.REQUEST_PROTOCOL	
O.TOKEN_GENERATION	
O.REQUEST_VERIFICATION	T.REQUEST_FORGERY, T.INCOHERENT_HASH
O.HASH_VERIFICATION	T.REQUEST_FORGERY, T.INCOHERENT_HASH
O.DEFAULT_POLICY	
O.NON_OPERATIONAL_CONTEXT_CREATION	T.CONTEXT_MODIFICATION
O.OPERATIONAL_CONTEXT_PROTECTION	T.CONTEXT_MODIFICATION
O.CONTEXTS_VISUALIZATION	
O.CONTEXT_STOP	T.CLOCK_MODIFICATION, T.KEYS_DISCLOSURE
O.INTERNAL_CLOCK	
O.CRYPTO	T.KEYS_DISCLOSURE
O.CERTIFICATE_IMPORTATION	
O.KEYS_EXPORT	T.KEYS_DISCLOSURE
O.KEYS_IMPORT	T.KEYS_DISCLOSURE
O.INTERRUPTION	T.POWER_STATE_MODIFICATION, T.SYNCHRO_STATE_MODIFICATION
O.SECURE_STATE_RETURN	T.TIME_GAP_HISTORY_MODIFICATION, T.POWER_STATE_MODIFICATION, T.SYNCHRO_STATE_MODIFICATION
O.ADMIN_AUTHENTICATION	T.CONTEXT_MODIFICATION, T.CLOCK_MODIFICATION, T.KEYS_DISCLOSURE, T.ADMIN_USURPATION, T.AUDIT_RECORDS_MODIFICATION
O.TIMESTAMPING_UNIT_LOGS	T.CLOCK_MODIFICATION
O.ADMINISTRATION_LOGS	T.CONTEXT_MODIFICATION, T.CLOCK_MODIFICATION, T.TIME_GAP_HISTORY_MODIFICATION, T.KEYS_DISCLOSURE, T.ADMIN_AUTH_DATA_DISCLOSURE, T.ADMIN_AUTH_DATA_MODIFICATION, T.POWER_STATE_MODIFICATION, T.SYNCHRO_STATE_MODIFICATION, T.ADMIN_USURPATION, T.AUDIT_RECORDS_MODIFICATION

Security objectives	Threats
O.AUDIT_RECORDS_PROTECTION	T.AUDIT_RECORDS_MODIFICATION
O.ALARMS	T.CONTEXT_MODIFICATION, T.CLOCK_MODIFICATION, T.TIME_GAP_HISTORY_MODIFICATION, T.KEYS_DISCLOSURE, T.ADMIN_AUTH_DATA_DISCLOSURE, T.ADMIN_AUTH_DATA_MODIFICATION, T.POWER_STATE_MODIFICATION, T.SYNCHRO_STATE_MODIFICATION, T.ADMIN_USURPATION, T.AUDIT_RECORDS_MODIFICATION
OE.TOKEN_VERIFICATION	
OE.ADMIN	T.ADMIN_AUTH_DATA_DISCLOSURE, T.ADMIN_AUTH_DATA_MODIFICATION
OE.LOCAL_ADMIN	T.ADMIN_AUTH_DATA_DISCLOSURE, T.ADMIN_AUTH_DATA_MODIFICATION
OE.CERTIFICATE_REQUEST	
OE.CERTIFICATE_IMPORT	
OE.AUDIT_RECORDS_ANALYSIS	
OE.TIMESTAMPING_ AUTHORITY	T.ADMIN_AUTH_DATA_DISCLOSURE, T.ADMIN_AUTH_DATA_MODIFICATION
OE.CERTIFICATION_AUTHORITY	
OE.PHYSICAL_PROTECTION	
OE.NETWORK	
OE.SUPERVISION	
OE.TIME_REFERENCE	T.CLOCK_MODIFICATION

Table 2 Security objectives coverage by Threats

Organisational security policies (OSP)	Security objectives	Rationale
OSP.SERVICES	O.CRYPTO, O.TOKEN_GENERATION, O.INTERNAL_CLOCK, O.INTERRUPTION	Section 7.1.2
OSP.CRYPTO	O.CRYPTO, O.TOKEN_GENERATION, O.ADMIN_AUTHENTICATION	Section 7.1.2
OSP.INTERNAL_CLOCK_SYNCHRONIZATION	O.INTERNAL_CLOCK, O.TIMESTAMPING_UNIT_LOGS, O.ADMIN_AUTHENTICATION, O.ADMINISTRATION_LOGS, O.ALARMS	Section 7.1.2
OSP.DEFAULT_POLICY	O.DEFAULT_POLICY	Section 7.1.2
OSP.CONTEXT_MANAGEMENT	O.CONTEXTS_VISUALIZATION, O.CONTEXT_STOP, O.NON_OPERATIONAL_CONTEXT_CREATION	Section 7.1.2
OSP.CERTIFICATE_IMPORTATION	O.CERTIFICATE_IMPORTATION	Section 7.1.2
OSP.REQUEST_PROTOCOL	O.REQUEST_PROTOCOL	Section 7.1.2

Table 3 Organisational security policies coverage by Security objectives

Security objectives	Organisational security policies (OSP)
O.REQUEST_PROTOCOL	OSP.REQUEST_PROTOCOL
O.TOKEN_GENERATION	OSP.SERVICES, OSP.CRYPTO
O.REQUEST_VERIFICATION	
O.HASH_VERIFICATION	
O.DEFAULT_POLICY	OSP.DEFAULT_POLICY
O.NON_OPERATIONAL_CONTEXT_CREATION	OSP.CONTEXT_MANAGEMENT
O.OPERATIONAL_CONTEXT_PROTECTION	
O.CONTEXTS_VISUALIZATION	OSP.CONTEXT_MANAGEMENT
O.CONTEXT_STOP	OSP.CONTEXT_MANAGEMENT
O.INTERNAL_CLOCK	OSP.SERVICES, OSP.INTERNAL_CLOCK_SYNCHRONIZATION
O.CRYPTO	OSP.SERVICES, OSP.CRYPTO
O.CERTIFICATE_IMPORTATION	OSP.CERTIFICATE_IMPORTATION
O.KEYS_EXPORT	
O.KEYS_IMPORT	
O.INTERRUPTION	OSP.SERVICES
O.SECURE_STATE_RETURN	
O.ADMIN_AUTHENTICATION	OSP.CRYPTO, OSP.INTERNAL_CLOCK_SYNCHRONIZATION
O.TIMESTAMPING_UNIT_LOGS	OSP.INTERNAL_CLOCK_SYNCHRONIZATION
O.ADMINISTRATION_LOGS	OSP.INTERNAL_CLOCK_SYNCHRONIZATION
O.AUDIT_RECORDS_PROTECTION	
O.ALARMS	OSP.INTERNAL_CLOCK_SYNCHRONIZATION
OE.TOKEN_VERIFICATION	
OE.ADMIN	
OE.LOCAL_ADMIN	
OE.CERTIFICATE_REQUEST	
OE.CERTIFICATE_IMPORT	
OE.AUDIT_RECORDS_ANALYSIS	
OE.TIMESTAMPING_ AUTHORITY	
OE.CERTIFICATION_AUTHORITY	

Security objectives	Organisational security policies (OSP)
OE.PHYSICAL_PROTECTION	
OE.NETWORK	
OE.SUPERVISION	
OE.TIME_REFERENCE	

Table 4 Security objectives coverage by OSP

Assumptions	Security objectives for operational environment	Rationale
A.TOKEN_VERIFICATION	OE.TOKEN_VERIFICATION	Section 7.1.3
A.ADMIN	OE.ADMIN	Section 7.1.3
A.AUDIT	OE.AUDIT_RECORDS_ANALYSIS	Section 7.1.3
A.CERTIFICATION_AUTHORITY	OE.CERTIFICATION_AUTHORITY, OE.CERTIFICATE_IMPORT	Section 7.1.3
A.TIME_STAMPING_AUTHORITY	OE.TIMESTAMPING_ AUTHORITY, OE.CERTIFICATE_REQUEST	Section 7.1.3
A.TIME_REFERENCE	OE.TIME_REFERENCE	Section 7.1.3
A.LOCATION	OE.PHYSICAL_PROTECTION, OE.NETWORK	Section 7.1.3
A.LOCAL_ADMIN	OE.LOCAL_ADMIN	Section 7.1.3
A.NETWORK	OE.NETWORK	Section 7.1.3
A.SUPERVISION	OE.SUPERVISION	Section 7.1.3

Table 5 Assumptions coverage by Security objectives for operational environment

Security objectives for operational environment	Assumptions
OE.TOKEN_VERIFICATION	A.TOKEN_VERIFICATION
OE.ADMIN	A.ADMIN
OE.LOCAL_ADMIN	A.LOCAL_ADMIN
OE.CERTIFICATE_REQUEST	A.TIME_STAMPING_AUTHORITY
OE.CERTIFICATE_IMPORT	A.CERTIFICATION_AUTHORITY
OE.AUDIT_RECORDS_ANALYSIS	A.AUDIT
OE.TIMESTAMPING_ AUTHORITY	A.TIME_STAMPING_AUTHORITY
OE.CERTIFICATION_AUTHORITY	A.CERTIFICATION_AUTHORITY
OE.PHYSICAL_PROTECTION	A.LOCATION
OE.NETWORK	A.LOCATION, A.NETWORK
OE.SUPERVISION	A.SUPERVISION
OE.TIME_REFERENCE	A.TIME_REFERENCE

Table 6 Security objectives for operational environment coverage by Assumptions

7.2 Security requirements rationale

7.2.1 Security objectives coverage

7.2.1.1 Security objectives for the TOE

Security objectives on awaited TOE services

O.REQUEST_PROTOCOL This objective is covered by the policy of time-stamp tokens generation (FDP_IFC.1/Timestamp_Token_Generation_Policy, FDP_IFF.1/Timestamp_Token_Generation_Policy, FMT_MSA.3/Default_Timestamping_Policy, FMT_MSA.3/Internal_Clock, FMT_MSA.3/Context, FMT_MSA.1/Default_Timestamping_Policy, FMT_MSA.1/Internal_Clock, FMT_MSA.1/Context and FMT_SMF.1/Context_Management_Policy, FMT_SMF.1/Default_Timestamping_Policy, FMT_SMF.1/Internal_Clock) which controls the requests of time-stamp tokens as well as the tokens delivered in return by the time-stamping system.

This objective is also covered by FDP_ITC.1/Timestamp_Token_Request and FDP_ETC.1/Timestamp_Token which refer to the policy of time-stamp tokens generation for the importation of the requests and the export of the tokens respectively. Moreover, FPT_TDC.1/Hash_Algorithms and FPT_TDC.1/Timestamping_Policies cover this objective because they guarantee the coherent interpretation of the identifiers of hash algorithms and time-stamp policies.

O.TOKEN_GENERATION This objective is covered by the policy of generation of tokens (FDP_ACC.1/Timestamp_Token_Generation_Policy, FDP_ACF.1/Timestamp_Token_Generation_Policy, FMT_MSA.3/Default_Timestamping_Policy, FMT_MSA.3/Internal_Clock, FMT_MSA.3/Context, FMT_MSA.3/Private_Key_Validity_Period, FMT_MSA.1/Default_Timestamping_Policy, FMT_MSA.1/Internal_Clock, FMT_MSA.1/Context, FMT_MSA.1/Private_Key_Validity_Period, FMT_SMF.1/Context_Management_Policy, FMT_SMF.1/Default_Timestamping_Policy, FMT_SMF.1/Internal_Clock and FMT_SMF.1/Private_Key_Validity_Period) which controls the operations of creation and signature of the time-stamp tokens. Moreover, this objective is also covered by FCS_COP.1/Timestamp_Token which provides the asymmetric cryptographic operation for the digital signature generation of the time-stamp tokens.

Objectives of security to protect the sensitive assets of the TOE

Management of the requests of time-stamp tokens

O.REQUEST_VERIFICATION This objective is covered by the policy of time-stamp tokens generation (FDP_IFC.1/Timestamp_Token_Generation_Policy, FDP_IFF.1/Timestamp_Token_Generation_Policy, FMT_MSA.3/Default_Timestamping_Policy, FMT_MSA.3/Internal_Clock, FMT_MSA.3/Context, FMT_MSA.1/Default_Timestamping_Policy, FMT_MSA.1/Internal_Clock, FMT_MSA.1/Context and FMT_SMF.1/Context_Management_Policy, FMT_SMF.1/Default_Timestamping_Policy, FMT_SMF.1/Internal_Clock) which prohibits the importation of requests whose format is not in conformance with the format awaited by the time-stamping system. This objective is also covered by FDP_ITC.1/Timestamp_Token_Request which refers to the policy of time-stamp tokens generation for the importation of the requests.

O.HASH_VERIFICATION This objective is covered by the policy of time-stamp tokens generation (FDP_IFC.1/Timestamp_Token_Generation_Policy, FDP_IFF.1/Timestamp_Token_Generation_Policy, FMT_MSA.3/Default_Timestamping_Policy, FMT_MSA.3/Internal_Clock, FMT_MSA.3/Context, FMT_MSA.1/Default_Timestamping_Policy, FMT_MSA.1/Internal_Clock, FMT_MSA.1/Context and FMT_SMF.1/Context_Management_Policy, FMT_SMF.1/Default_Timestamping_Policy, FMT_SMF.1/Internal_Clock) which controls the requests of time-stamp tokens by checking in particular that the digest length of document to time-stamp is coherent with the identifier of the referred hash algorithm, and that this algorithm is authorized by the applied time-stamp policy. This objective is also covered by FDP_ITC.1/Timestamp_Token_Request which refers to the policy of time-stamp tokens generation for the importation of the requests. Moreover, FPT_TDC.1/Hash_Algorithms covers this objective because it guarantees the coherent interpretation of the identifiers of hash algorithms.

O.DEFAULT_POLICY This objective is covered by FMT_SMF.1/Default_Timestamping_Policy which allows to lay down the default time-stamp policy and the hash algorithms admitted for this policy, and by FDP_ITC.1/Default_Timestamping_Policy for the importation of the reference of this default time-stamp policy by the Security administrator. Moreover, FPT_TDC.1/Hash_Algorithms and FPT_TDC.1/Timestamping_Policies cover this objective

because they guarantee the coherent interpretation of the identifiers of hash algorithms and time-stamp policies.

Management of the time-stamping contexts

O.NON_OPERATIONAL_CONTEXT_CREATION This objective is covered by the management policy of the time-stamping contexts (FDP_ACC.1/Context_Management_Policy, FDP_ACF.1/Context_Management_Policy, FMT_MSA.1/Context, FMT_MSA.3/Context, FMT_SMF.1/Context, and FDP_SDI.2/Context) which controls in particular the operations of creation and modification of the non operational time-stamping contexts. This objective is also covered by FDP_ITC.1/Context which refers to the management policy of the time-stamping contexts for the importation of the necessary information to the creation of non operational time-stamping contexts.

O.OPERATIONAL_CONTEXT_PROTECTION This objective is covered by the management policy of the time-stamping contexts (FDP_ACC.1/Context_Management_Policy, FDP_ACF.1/Context_Management_Policy, FMT_MSA.1/Context, FMT_MSA.3/Context, FMT_SMF.1/Context and FDP_SDI.2/Context) which controls in particular the operations of modification and destruction of the time-stamping contexts.

O.CONTEXTS_VISUALIZATION This objective is covered by the management policy of the time-stamping contexts (FDP_ACC.1/Context_Management_Policy, FDP_ACF.1/Context_Management_Policy, FMT_MSA.1/Context, FMT_MSA.3/Context and FMT_SMF.1/Context_Management_Policy) which controls in particular the operation of consultation of the time-stamping contexts.

O.CONTEXT_STOP This objective is covered by the management policy of the time-stamping contexts (FDP_ACC.1/Context_Management_Policy, FDP_ACF.1/Context_Management_Policy, FMT_MSA.1/Context, FMT_MSA.3/Context and FMT_SMF.1/Context_Management_Policy) which controls in particular the operation of destruction of the time-stamping contexts. Moreover, this objective is also covered by FPT_PHP.1 and FPT_PHP.3 which guarantee the detection of physical intrusions.

Management of synchronization

O.INTERNAL_CLOCK This objective is covered by FMT_MTD.1/Internal_Clock which guarantees that the time-stamping unit internal clock is initially synchronized by a Security administrator during the initialization of the time-stamping unit and by FMT_SMF.1/Internal_Clock which ensures that the monitoring of the drift and the maintenance of synchronization with UTC time are carried out by the TOE according to the guaranteed accuracy. This objective is also covered by FDP_ITC.1/Internal_Clock which refers to the policy of generation of the time-stamp tokens with regard to the synchronization of the internal clock of the time-stamping unit with UTC. FMT_MSA.1/Internal_Clock and FMT_MSA.3/Internal_Clock also cover this objective because they limit the possibility of modifying the current state of synchronization to a Security administrator authenticated and to the TOE itself and FPT_STM.1 ensures that the date associated with each audit event is reliable.

Cryptographic key management

O.CRYPTO This objective is covered by all the requirements concerning the cryptographic key management and operations: FCS_COP.1/Timestamp_Token, FCS_CKM.1/Context_Keys, FCS_CKM.4/Context_Keys, and FMT_MSA.2/Context_Keys.

O.CERTIFICATE_IMPORTATION This objective is covered by the key management policy (FDP_IFC.1/Key_Management_Policy, FDP_IFF.1/Key_Management_Policy, FMT_MSA.1/Private_Key_Validity_Period, FMT_MSA.1/Context, FMT_MSA.3/Private_Key_Validity_Period, FMT_MSA.3/Context, FMT_SMF.1/Private_Key_Validity_Period and FMT_SMF.1/Context_Management_Policy) which controls the export of the key pairs generated by the TOE and the importation of the certificates of time-stamping unit.

This objective is also covered by FDP_ETC.1/Non_Operational_Context_Public_Key and FDP_ITC.2/Timestamping_Unit_Certificate which refer to the key management policy for the export of the public-key of a non operational time-stamping context and the importation of the corresponding certificate, and by FPT_TDC.1/Timestamping_Unit_Certificate which guarantees the coherent interpretation of certain fields of the certificate, in particular the value of the public-key. Moreover, FTP_TRP.1/Timestamping_Unit_Certificate imposes a path of confidence with the Security administrator at the time of the importation of the certificates of time-stamping unit.

O.KEYS_EXPORT This objective is covered by the key management policy (FDP_IFC.1/Key_Management_Policy and FDP_IFF.1/Key_Management_Policy) which controls the export of the private keys generated by the TOE.

O.KEYS_IMPORT This objective is covered by the key management policy (FDP_IFC.1/Key_Management_Policy and FDP_IFF.1/Key_Management_Policy) which controls the importation of private keys or key pairs generated outside of the TOE.

Time-stamping unit stop

O.INTERRUPTION This objective is covered by FMT_SMF.1/Temporary_Interruption which guarantees the supervision of the states of synchronization and power and ensures the stop of the services of time-stamping in the event of loss of synchronization of the internal clock and cut of external power.

O.SECURE_STATE_RETURN This objective is covered by FPT_RCV.2 which guarantees that the TOE can return in a secure operational state following a loss of external power and a loss of synchronization of the internal clock which causes the stop of the services of time-stamping in an automatic way or with the help of a Security administrator. Moreover, this objective is also covered by FPT_TST.1 which ensures that tests must be carried out by the TOE following a temporary interruption of the services of time-stamping.

Administration

O.ADMIN_AUTHENTICATION This objective is covered by FIA_UID.2 and FIA_UAU.2 which require the identification and the authentication of the Security administrators and the Auditors before carrying out any operation of administration or audit. Moreover, this

objective is also covered by FMT_SMR.1 which requires the maintenance of the various roles by the TOE.

Audits and alarms

O.TIMESTAMPING_UNIT_LOGS This objective is covered by FAU_GEN.1/Internal_Clock which ensures the generation of audit events for the operations of synchronization of the internal clock and by FPT_STM.1 which ensures that the date associated with each audit event is reliable. Moreover, this objective is also covered by FAU_SAR.1 and FAU_SAR.3 which provide the consultation of the audit events.

O.ADMINISTRATION_LOGS This objective is covered by FAU_GEN.1/Administration which ensures the generation of audit events concerning the operations of administration and by FPT_STM.1 which ensures that the date associated with each audit event is reliable. Moreover, this objective is also covered by FAU_SAR.1 and FAU_SAR.3 which provide the consultation of the audit events.

O.AUDIT_RECORDS_PROTECTION This objective is covered by FAU_STG.1, FAU_STG.2 and FAU_STG.4 which protect in integrity and in availability the audit events.

O.ALARMS This objective is covered by FAU_ARP.1/Security_Alarm which requires to raise a security alarm when a potential violation of security is detected and by FAU_SAA.1/Security_Alarm which indicates the rules used to detect these potential violations.

7.2.2 Coverage table between objectives and security requirements

Security objectives	Functional requirement for the TOE	Rationale
O.REQUEST_PROTOCOL	FDP_ETC.1/Timestamp_Token, FDP_IFC.1/Timestamp_Token_Generation_Policy, FDP_IFF.1/Timestamp_Token_Generation_Policy, FPT_TDC.1/Hash_Algorithms, FDP_ITC.1/Timestamp_Token_Request, FPT_TDC.1/Timestamping_Policies, FMT_MSA.3/Internal_Clock, FMT_SMF.1/Internal_Clock, FMT_MSA.3/Context, FMT_MSA.3/Default_Timestamping_Policy, FMT_MSA.1/Context, FMT_MSA.1/Default_Timestamping_Policy, FMT_MSA.1/Internal_Clock, FMT_SMF.1/Context, FMT_SMF.1/Default_Timestamping_Policy	Section 7.2.1

Security objectives	Functional requirement for the TOE	Rationale
O.TOKEN_GENERATION	FCS_COP.1/Timestamp_Token, FDP_ACC.1/Timestamp_Token_Generation_Policy, FDP_ACF.1/Timestamp_Token_Generation_Policy, FMT_MSA.3/Internal_Clock, FMT_SMF.1/Internal_Clock, FMT_MSA.3/Context, FMT_MSA.3/Private_Key_Validity_Period, FMT_MSA.3/Default_Timestamping_Policy, FMT_MSA.1/Context, FMT_SMF.1/Context, FMT_MSA.1/Private_Key_Validity_Period, FMT_SMF.1/Private_Key_Validity_Period, FMT_MSA.1/Default_Timestamping_Policy, FMT_MSA.1/Internal_Clock, FMT_SMF.1/Default_Timestamping_Policy	Section 7.2.1
O.REQUEST_VERIFICATION	FDP_IFC.1/Timestamp_Token_Generation_Policy, FDP_IFF.1/Timestamp_Token_Generation_Policy, FMT_MSA.3/Internal_Clock, FDP_ITC.1/Timestamp_Token_Request, FMT_SMF.1/Internal_Clock, FMT_MSA.3/Context, FMT_MSA.1/Context, FMT_SMF.1/Context, FMT_MSA.3/Default_Timestamping_Policy, FMT_MSA.1/Default_Timestamping_Policy, FMT_MSA.1/Internal_Clock, FMT_SMF.1/Default_Timestamping_Policy	Section 7.2.1
O.HASH_VERIFICATION	FPT_TDC.1/Hash_Algorithms, FDP_IFC.1/Timestamp_Token_Generation_Policy, FDP_IFF.1/Timestamp_Token_Generation_Policy, FMT_MSA.3/Internal_Clock, FDP_ITC.1/Timestamp_Token_Request, FMT_SMF.1/Internal_Clock, FMT_MSA.3/Context, FMT_MSA.1/Context, FMT_SMF.1/Context, FMT_MSA.3/Default_Timestamping_Policy, FMT_MSA.1/Default_Timestamping_Policy, FMT_MSA.1/Internal_Clock, FMT_SMF.1/Default_Timestamping_Policy	Section 7.2.1

Security objectives	Functional requirement for the TOE	Rationale
O.DEFAULT_POLICY	FMT_SMF.1/Default_Timestamping_Policy, FPT_TDC.1/Timestamping_Policies, FPT_TDC.1/Hash_Algorithms, FDP_ITC.1/Default_Timestamping_Policy	Section 7.2.1
O.NON_OPERATIONAL_CONTEXT_CREATION	FDP_ACC.1/Context_Management_Policy, FDP_ACF.1/Context_Management_Policy, FMT_MSA.3/Context, FMT_SMF.1/Context, FMT_MSA.1/Context, FDP_SDI.2/Context, FDP_ITC.1/Context	Section 7.2.1
O.OPERATIONAL_CONTEXT_PROTECTION	FDP_ACC.1/Context_Management_Policy, FDP_ACF.1/Context_Management_Policy, FMT_MSA.3/Context, FMT_SMF.1/Context, FMT_MSA.1/Context, FDP_SDI.2/Context	Section 7.2.1
O.CONTEXTS_VISUALIZATION	FDP_ACC.1/Context_Management_Policy, FDP_ACF.1/Context_Management_Policy, FMT_SMF.1/Context, FMT_MSA.3/Context, FMT_MSA.1/Context	Section 7.2.1
O.CONTEXT_STOP	FDP_ACC.1/Context_Management_Policy, FDP_ACF.1/Context_Management_Policy, FPT_PHP.1, FPT_PHP.3, FMT_SMF.1/Context, FMT_MSA.3/Context, FMT_MSA.1/Context	Section 7.2.1
O.INTERNAL_CLOCK	FMT_MSA.3/Internal_Clock, FMT_SMF.1/Internal_Clock, FMT_MSA.1/Internal_Clock, FMT_MTD.1/Internal_Clock, FDP_ITC.1/Internal_Clock, FPT_STM.1	Section 7.2.1
O.CRYPTO	FCS_CKM.4/Context_Keys, FCS_COP.1/Timestamp_Token, FCS_CKM.1/Context_Keys, FMT_MSA.2/Context_Keys	Section 7.2.1

Security objectives	Functional requirement for the TOE	Rationale
O.CERTIFICATE_IMPORTATION	FDP_ITC.2/Timestamping_Unit_Certificate, FDP_IFC.1/Key_Management_Policy, FDP_IFF.1/Key_Management_Policy, FPT_TDC.1/Timestamping_Unit_Certificate, FDP_ETC.1/Non_Operational_Context_Public_Key, FTP_TRP.1/Timestamping_Unit_Certificate, FMT_SMF.1/Private_Key_Validity_Period, FMT_MSA.3/Context, FMT_MSA.1/Context, FMT_SMF.1/Context, FMT_MSA.3/Private_Key_Validity_Period, FMT_MSA.1/Private_Key_Validity_Period	Section 7.2.1
O.KEYS_EXPORT	FDP_IFC.1/Key_Management_Policy, FDP_IFF.1/Key_Management_Policy	Section 7.2.1
O.KEYS_IMPORT	FDP_IFC.1/Key_Management_Policy, FDP_IFF.1/Key_Management_Policy	Section 7.2.1
O.INTERRUPTION	FMT_SMF.1/Temporary_Interruption	Section 7.2.1
O.SECURE_STATE_RETURN	FPT_TST.1, FPT_RCV.2	Section 7.2.1
O.ADMIN_AUTHENTICATION	FIA_UID.2, FIA_UAU.2, FMT_SMR.1	Section 7.2.1
O.TIMESTAMPING_UNIT_LOGS	FAU_GEN.1/Internal_Clock, FPT_STM.1, FAU_SAR.1, FAU_SAR.3	Section 7.2.1
O.ADMINISTRATION_LOGS	FAU_GEN.1/Administration, FAU_SAR.1, FAU_SAR.3, FPT_STM.1	Section 7.2.1
O.AUDIT_RECORDS_PROTECTION	FAU_STG.1, FAU_STG.4, FAU_STG.2	Section 7.2.1
O.ALARMS	FAU_ARP.1/Security_Alarm, FAU_SAA.1/Security_Alarm	Section 7.2.1

Table 7 Security objectives for the TOE coverage by functional requirements

Functional requirement for the TOE	Security objectives
FDP_ACC.1/Context_Management_Policy	O.NON_OPERATIONAL_CONTEXT_CREATION, O.OPERATIONAL_CONTEXT_PROTECTION, O.CONTEXTS_VISUALIZATION, O.CONTEXT_STOP
FDP_ACF.1/Context_Management_Policy	O.NON_OPERATIONAL_CONTEXT_CREATION, O.OPERATIONAL_CONTEXT_PROTECTION, O.CONTEXTS_VISUALIZATION, O.CONTEXT_STOP
FMT_MSA.3/Context	O.REQUEST_PROTOCOL, O.TOKEN_GENERATION, O.REQUEST_VERIFICATION, O.HASH_VERIFICATION, O.NON_OPERATIONAL_CONTEXT_CREATION, O.OPERATIONAL_CONTEXT_PROTECTION, O.CONTEXTS_VISUALIZATION, O.CONTEXT_STOP, O.CERTIFICATE_IMPORTATION
FMT_MSA.1/Context	O.REQUEST_PROTOCOL, O.TOKEN_GENERATION, O.REQUEST_VERIFICATION, O.HASH_VERIFICATION, O.NON_OPERATIONAL_CONTEXT_CREATION, O.OPERATIONAL_CONTEXT_PROTECTION, O.CONTEXTS_VISUALIZATION, O.CONTEXT_STOP, O.CERTIFICATE_IMPORTATION
FMT_SMF.1/Context	O.REQUEST_PROTOCOL, O.TOKEN_GENERATION, O.REQUEST_VERIFICATION, O.HASH_VERIFICATION, O.NON_OPERATIONAL_CONTEXT_CREATION, O.OPERATIONAL_CONTEXT_PROTECTION, O.CONTEXTS_VISUALIZATION, O.CONTEXT_STOP, O.CERTIFICATE_IMPORTATION
FDP_ITC.1/Context	O.NON_OPERATIONAL_CONTEXT_CREATION
FDP_SDI.2/Context	O.NON_OPERATIONAL_CONTEXT_CREATION, O.OPERATIONAL_CONTEXT_PROTECTION
FDP_ETC.1/Non_Operational_Context_Public_Key	O.CERTIFICATE_IMPORTATION
FDP_ITC.2/Timestamping_Unit_Certificate	O.CERTIFICATE_IMPORTATION
FPT_TDC.1/Timestamping_Unit_Certificate	O.CERTIFICATE_IMPORTATION
FTP_TRP.1/Timestamping_Unit_Certificate	O.CERTIFICATE_IMPORTATION
FDP_IFC.1/Key_Management_Policy	O.CERTIFICATE_IMPORTATION, O.KEYS_EXPORT, O.KEYS_IMPORT

Functional requirement for the TOE	Security objectives
FDP_IFF.1/Key_Management_Policy	O.CERTIFICATE_IMPORTATION, O.KEYS_EXPORT, O.KEYS_IMPORT
FMT_MSA.3/Private_Key_Validity_Period	O.TOKEN_GENERATION, O.CERTIFICATE_IMPORTATION
FMT_MSA.1/Private_Key_Validity_Period	O.TOKEN_GENERATION, O.CERTIFICATE_IMPORTATION
FMT_SMF.1/Private_Key_Validity_Period	O.TOKEN_GENERATION, O.CERTIFICATE_IMPORTATION
FCS_CKM.1/Context_Keys	O.CRYPTO
FCS_CKM.4/Context_Keys	O.CRYPTO
FMT_MSA.2/Context_Keys	O.CRYPTO
FDP_ITC.1/Timestamp_Token_Request	O.REQUEST_PROTOCOL, O.REQUEST_VERIFICATION, O.HASH_VERIFICATION
FDP_ETC.1/Timestamp_Token	O.REQUEST_PROTOCOL
FDP_IFC.1/Timestamp_Token_Generation_Policy	O.REQUEST_PROTOCOL, O.REQUEST_VERIFICATION, O.HASH_VERIFICATION
FDP_IFF.1/Timestamp_Token_Generation_Policy	O.REQUEST_PROTOCOL, O.REQUEST_VERIFICATION, O.HASH_VERIFICATION
FMT_MSA.3/Default_Timestamping_Policy	O.REQUEST_PROTOCOL, O.TOKEN_GENERATION, O.REQUEST_VERIFICATION, O.HASH_VERIFICATION
FMT_MSA.3/Internal_Clock	O.REQUEST_PROTOCOL, O.TOKEN_GENERATION, O.REQUEST_VERIFICATION, O.HASH_VERIFICATION, O.INTERNAL_CLOCK
FMT_MSA.1/Default_Timestamping_Policy	O.REQUEST_PROTOCOL, O.TOKEN_GENERATION, O.REQUEST_VERIFICATION, O.HASH_VERIFICATION
FMT_MSA.1/Internal_Clock	O.REQUEST_PROTOCOL, O.TOKEN_GENERATION, O.REQUEST_VERIFICATION, O.HASH_VERIFICATION, O.INTERNAL_CLOCK
FDP_ACC.1/Timestamp_Token_Generation_Policy	O.TOKEN_GENERATION
FDP_ACF.1/Timestamp_Token_Generation_Policy	O.TOKEN_GENERATION
FCS_COP.1/Timestamp_Token	O.TOKEN_GENERATION, O.CRYPTO

Functional requirement for the TOE	Security objectives
FMT_SMF.1/Default_Timestamping_Policy	O.REQUEST_PROTOCOL, O.TOKEN_GENERATION, O.REQUEST_VERIFICATION, O.HASH_VERIFICATION, O.DEFAULT_POLICY
FDP_ITC.1/Default_Timestamping_Policy	O.DEFAULT_POLICY
FMT_SMF.1/Internal_Clock	O.REQUEST_PROTOCOL, O.TOKEN_GENERATION, O.REQUEST_VERIFICATION, O.HASH_VERIFICATION, O.INTERNAL_CLOCK
FMT_MTD.1/Internal_Clock	O.INTERNAL_CLOCK
FDP_ITC.1/Internal_Clock	O.INTERNAL_CLOCK
FMT_SMF.1/Temporary_Interruption	O.INTERRUPTION
FPT_TDC.1/Hash_Algorithms	O.REQUEST_PROTOCOL, O.HASH_VERIFICATION, O.DEFAULT_POLICY
FPT_TDC.1/Timestamping_Policies	O.REQUEST_PROTOCOL, O.DEFAULT_POLICY
FPT_PHP.1	O.CONTEXT_STOP
FPT_PHP.3	O.CONTEXT_STOP
FMT_SMR.1	O.ADMIN_AUTHENTICATION
FIA_UID.2	O.ADMIN_AUTHENTICATION
FIA_UAU.2	O.ADMIN_AUTHENTICATION
FPT_TST.1	O.SECURE_STATE_RETURN
FPT_RCV.2	O.SECURE_STATE_RETURN
FAU_GEN.1/Internal_Clock	O.TIMESTAMPING_UNIT_LOGS
FAU_GEN.1/Administration	O.ADMINISTRATION_LOGS
FAU_SAR.1	O.TIMESTAMPING_UNIT_LOGS, O.ADMINISTRATION_LOGS
FAU_SAR.3	O.TIMESTAMPING_UNIT_LOGS, O.ADMINISTRATION_LOGS
FAU_STG.1	O.AUDIT_RECORDS_PROTECTION
FAU_ARP.1/Security_Alarm	O.ALARMS
FAU_SAA.1/Security_Alarm	O.ALARMS
FPT_STM.1	O.INTERNAL_CLOCK, O.TIMESTAMPING_UNIT_LOGS, O.ADMINISTRATION_LOGS
FAU_STG.4	O.AUDIT_RECORDS_PROTECTION
FAU_STG.2	O.AUDIT_RECORDS_PROTECTION

Table 8 Functional requirements coverage by Security objectives for the TOE

7.3 Security requirements dependencies

7.3.1 Dependencies of functional security requirements

Requirements	CC Dependencies	Satisfied Dependencies
FDP_ACC.1/Context_Management_Policy	(FDP_ACF.1)	FDP_ACF.1/Context_Management_Policy
FDP_ACF.1/Context_Management_Policy	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/Context_Management_Policy, FMT_MSA.3/Context
FMT_MSA.3/Context	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/Context, FMT_SMR.1
FMT_MSA.1/Context	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/Context_Management_Policy, FMT_SMF.1/Context, FDP_IFC.1/Key_Management_Policy, FDP_IFC.1/Timestamp_Token_Generation_Policy, FDP_ACC.1/Timestamp_Token_Generation_Policy, FMT_SMR.1
FMT_SMF.1/Context	No dependence	
FDP_ITC.1/Context	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.3)	FDP_ACC.1/Context_Management_Policy, FMT_MSA.3/Context
FDP_SDI.2/Context	No dependence	
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) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FPT_TDC.1/Timestamping_Unit_Certificate, FTP_TRP.1/Timestamping_Unit_Certificate, FDP_IFC.1/Key_Management_Policy
FPT_TDC.1/Timestamping_Unit_Certificate	No dependence	
FTP_TRP.1/Timestamping_Unit_Certificate	No dependence	
FDP_IFC.1/Key_Management_Policy	(FDP_IFF.1)	FDP_IFF.1/Key_Management_Policy
FDP_IFF.1/Key_Management_Policy	(FDP_IFC.1) and (FMT_MSA.3)	FMT_MSA.3/Context, FDP_IFC.1/Key_Management_Policy, FMT_MSA.3/Private_Key_Validity_Period

Requirements	CC Dependencies	Satisfied Dependencies
FMT_MSA.3/Private_Key_Validity_Period	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/Private_Key_Validity_Period, FMT_SMR.1
FMT_MSA.1/Private_Key_Validity_Period	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_IFC.1/Key_Management_Policy, FMT_SMF.1/Private_Key_Validity_Period, FDP_IFC.1/Timestamp_Token_Generation_Policy, FDP_ACC.1/Timestamp_Token_Generation_Policy, FMT_SMR.1
FMT_SMF.1/Private_Key_Validity_Period	No dependence	
FCS_CKM.1/Context_Keys	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.4/Context_Keys, FCS_COP.1/Timestamp_Token
FCS_CKM.4/Context_Keys	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FCS_CKM.1/Context_Keys
FMT_MSA.2/Context_Keys	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.1) and (FMT_SMR.1)	FDP_IFC.1/Key_Management_Policy, FMT_MSA.1/Private_Key_Validity_Period, FMT_SMR.1
FDP_ITC.1/Timestamp_Token_Request	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/Timestamp_Token_Generation_Policy, FMT_MSA.3/Internal_Clock
FDP_ETC.1/Timestamp_Token	(FDP_ACC.1 or FDP_IFC.1)	FDP_IFC.1/Timestamp_Token_Generation_Policy
FDP_IFC.1/Timestamp_Token_Generation_Policy	(FDP_IFF.1)	FDP_IFF.1/Timestamp_Token_Generation_Policy
FDP_IFF.1/Timestamp_Token_Generation_Policy	(FDP_IFC.1) and (FMT_MSA.3)	FMT_MSA.3/Context, FDP_IFC.1/Timestamp_Token_Generation_Policy, FMT_MSA.3/Default_Timestamping_Policy, FMT_MSA.3/Internal_Clock
FMT_MSA.3/Default_Timestamping_Policy	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/Default_Timestamping_Policy, FMT_SMR.1
FMT_MSA.3/Internal_Clock	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/Internal_Clock, FMT_SMR.1

Requirements	CC Dependencies	Satisfied Dependencies
FMT_MSA.1/Default_Timestamping_Policy	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_IFC.1/Timestamp_Token_Generation_Policy, FDP_ACC.1/Timestamp_Token_Generation_Policy, FMT_SMF.1/Default_Timestamping_Policy, FMT_SMR.1
FMT_MSA.1/Internal_Clock	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_IFC.1/Timestamp_Token_Generation_Policy, FDP_ACC.1/Timestamp_Token_Generation_Policy, FMT_SMF.1/Internal_Clock, FMT_SMR.1
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) and (FMT_MSA.3)	FMT_MSA.3/Context, FMT_MSA.3/Private_Key_Validity_Period, FMT_MSA.3/Default_Timestamping_Policy, FMT_MSA.3/Internal_Clock, FDP_ACC.1/Timestamp_Token_Generation_Policy
FCS_COP.1/Timestamp_Token	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/Context_Keys, FCS_CKM.4/Context_Keys
FMT_SMF.1/Default_Timestamping_Policy	No dependence	
FDP_ITC.1/Default_Timestamping_Policy	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/Timestamp_Token_Generation_Policy, FMT_MSA.3/Default_Timestamping_Policy
FMT_SMF.1/Internal_Clock	No dependence	
FMT_MTD.1/Internal_Clock	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1/Internal_Clock, FMT_SMR.1
FDP_ITC.1/Internal_Clock	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.3)	FMT_MSA.3/Internal_Clock, FDP_ACC.1/Timestamp_Token_Generation_Policy
FMT_SMF.1/Temporary_Interruption	No dependence	
FPT_TDC.1/Hash_Algorithms	No dependence	
FPT_TDC.1/Timestamping_Policies	No dependence	

Requirements	CC Dependencies	Satisfied Dependencies
FPT_PHP.1	No dependence	
FPT_PHP.3	No dependence	
FMT_SMR.1	(FIA_UID.1)	FIA_UID.2
FIA_UID.2	No dependence	
FIA_UAU.2	(FIA_UID.1)	FIA_UID.2
FPT_TST.1	No dependence	
FPT_RCV.2	(AGD_OPE.1)	AGD_OPE.1
FAU_GEN.1/Internal_Clock	(FPT_STM.1)	FPT_STM.1
FAU_GEN.1/Administration	(FPT_STM.1)	FPT_STM.1
FAU_SAR.1	(FAU_GEN.1)	FAU_GEN.1/Internal_Clock, FAU_GEN.1/Administration
FAU_SAR.3	(FAU_SAR.1)	FAU_SAR.1
FAU_STG.1	(FAU_GEN.1)	FAU_GEN.1/Internal_Clock, FAU_GEN.1/Administration
FAU_ARP.1/Security_Alarm	(FAU_SAA.1)	FAU_SAA.1/Security_Alarm
FAU_SAA.1/Security_Alarm	(FAU_GEN.1)	FAU_GEN.1/Internal_Clock, FAU_GEN.1/Administration
FPT_STM.1	No dependence	
FAU_STG.4	(FAU_STG.1)	FAU_STG.1
FAU_STG.2	(FAU_GEN.1)	FAU_GEN.1/Internal_Clock, FAU_GEN.1/Administration

Table 9 Functional Requirements Dependencies

7.3.2 Security assurance requirements dependencies

Requirements	CC Dependencies	Satisfied Dependencies
ADV_ARC.1	(ADV_FSP.1) and (ADV_TDS.1)	ADV_FSP.3, ADV_TDS.2
ADV_FSP.3	(ADV_TDS.1)	ADV_TDS.2
ADV_TDS.2	(ADV_FSP.3)	ADV_FSP.3
AGD_OPE.1	(ADV_FSP.1)	ADV_FSP.3
AGD_PRE.1	No dependence	
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 dependence	
ALC_DEL.1	No dependence	
ALC_DVS.1	No dependence	
ALC_FLR.3	No dependence	
ALC_LCD.1	No dependence	
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 dependence	
ASE_INT.1	No dependence	
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 dependence	
ASE_TSS.1	(ADV_FSP.1) and (ASE_INT.1) and (ASE_REQ.1)	ADV_FSP.3, ASE_INT.1, ASE_REQ.2
ATE_COV.2	(ADV_FSP.2) and (ATE_FUN.1)	ADV_FSP.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.3, AGD_OPE.1, AGD_PRE.1, ATE_COV.2, ATE_FUN.1
ATE_DPT.1	(ADV_ARC.1) and (ADV_TDS.2) and (ATE_FUN.1)	ADV_ARC.1, ADV_TDS.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.3, AGD_OPE.1, AGD_PRE.1

Table 10 Security Assurance Requirements dependencies

7.3.2.1 Rationale for unsatisfied dependencies

Dependence ADV_IMP.1 of AVA_VAN.3 is not supported. The dependence with ADV_IMP.1 is not satisfied because this requirement is covered by the component AVA_VAN.3.

Dependence ADV_TDS.3 of AVA_VAN.3 is not supported. The dependence with ADV_TDS.3 is not satisfied because this requirement is covered by the component AVA_VAN.3.

7.4 Evaluation assurance level rationale

The assurance level of this PP is EAL3+, because it is required by DCSSI *standard qualification* process [QUA-STD].

7.5 EAL augmentation rationale

7.5.1 AVA_VAN.3 Focused vulnerability analysis

Augmentation required by the *standard qualification* process.

7.5.2 ALC_FLR.3 Systematic flaw remediation

Augmentation required by the *standard qualification* process.

Appendix A Glossary

This Appendix gives definition of the main words used in this document. For the Common Criteria definition, refer to [CC1], § 4.

Certification Authority	Authority which issues public key certificates after verification of a person's identity or an other authority named in the certificate.
Coordinated Universal Time (UTC)	Time scale based on the second as defined in ITU-R Recommendation TF.460-5.
Internal clock	Clock used as time source to obtain the value of time to be contained in the time-stamp token.
Non operational time-stamping context	Set including the following information: • the identification of the synchronized time source with UTC which will be used to obtain the value of time to be contained in the time-stamp token, • the accuracy with UTC time that is guaranteed for the time contained in time-stamp tokens • the key pair value (and the identifier of the algorithm), • the private key validity period, • the reference(s) of supported time-stamp policies, • The identifier(s) of authorized hash algorithms for each time-stamp policy.
Operational time-stamping context	Set including the non operational time-stamping context information and the following additional information : • the effective validity period of the private key associated with the operational context, • The time-stamping unit certificate.
Time reference	Local UTC time approximation obtained from one or several time source whose accuracy is know with one or several UTC(k) sources.
Time-stamp token	Data object that binds a data digest to a particular time expressed in UTC time, establishing evidence that this data existed well before that time.
Time-stamp policy	Set of rules that indicate the applicability of a time-stamp token to a particular community and/or a class of application with common security requirements.

Time-Stamping Authority (TSA)	Authority responsible for the management of the time-stamping service.
Time-stamping services	Set of necessary services to generate time-stamp token and manage time-stamping unit.
Time-stamping System	Set of time-stamping unit and administration and supervision components used to provide time-stamping services.
Time-stamping unit	Set of hardware and software creating time-stamp tokens and identifiable by a name defined by the time-stamping authority (TSA) and a Certification Authority (CA). A time-stamping unit uses information of an operational context and the value of an internal clock synchronized with UTC.
UTC(k)	Time scale provided by the "k" laboratory and finely synchronized with UTC, with the goal to reach a precision of ±100 ns.

Index

T