Timestamping Policy

Universign Trust Network

7, rue du Faubourg Poissonnière, 75009 Paris, France

OID: 1.3.6.1.4.1.15819.5.2.(2/3)

VERSION : 2.2	DIFFUSION :PUBLIC	Effective date : 15/05/2019

Contents

1 Introduction

1.1 Overview

This Timestamping Policy defines the commitments of members of the UTN, for the issuance and management of Timestamps.

1.1.1 Presentation of the Universign Trust Network

The Universign Trust Network (UTN) is a network of Certification Authorities (CA) and Timestamping Authorities (TSA) governed by common policies defined by Cryptolog International.

In this document, the term UTN refers, based on its context of use, to the Universign Trust Network or to Cryptolog International, the company in charge of its control and management.

The UTN particularly comprises:

- Primary Certification Authorities (Primary CAs);
- Intermediate Certification Authorities (Intermediate CAs);
- Timestamping Certification Authorities (Timestamping CAs);
- Timestamping Authorities (TSAs);
- Certificate Subscribers;
- Relying Parties.

1.1.2 Organisation of the Universign Trust Network

The Certification Authorities operate according to a hierarchically structured chain of trust. The Primary CAs issue Certificates to the Intermediate CAs who, in turn, issue Certificates to natural persons or legal persons (the Subscribers). The Timestamping Units (TSU) of the Timestamping Authorities (TSAs) receive Certificates from the Timestamping CAs and issue Timestamps. The Timestamping CAs may receive Certificates from the Primary CAs.

The Relying Parties rely on the information contained in the Certificates of the Subscribers and the Timestamps.

The UTN:

- publishes the Certification Policy governing the CAs;
- publishes the Timestamping Policy governing the TSAs;

- manages the Primary CAs of the network.

The members of UTN:

- publish their Practice Statements;
- manage the CAs and TSAs associated with the services that they offer.

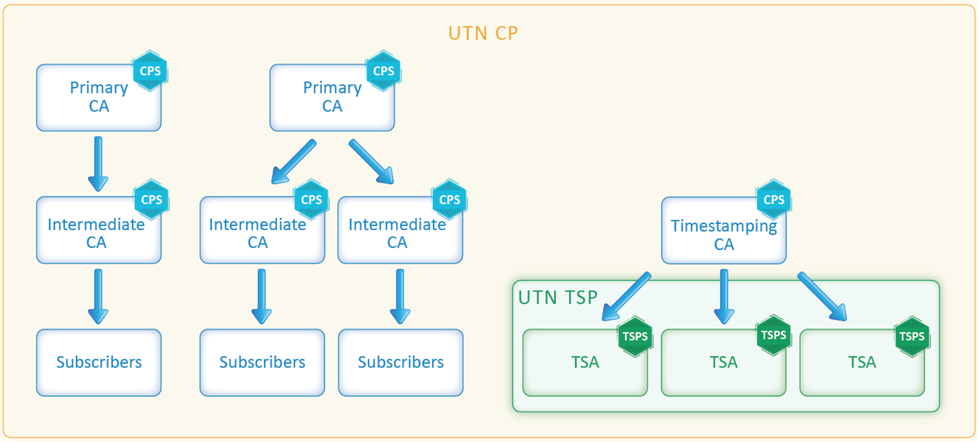

Figure 1: Organisation of the UTN

The UTN ensures the validation, management and application of the CP and the TSP. The UTN also ensures the consistency of the documentary references (User Agreement, CPS, TSPS, etc.) associated with its Policies. Every member authority of the UTN defines one or more Practice Statements in accordance with UTN 's Policy.

All requests of membership to the network or revocation of a Certificate of a CA or a TSU from the network must be addressed to the UTN. The components of the application file for membership to the network or revocation are communicated by UTN to the eligible bodies that request them.

The UTN monitors the audits and/or compliance controls conducted by members of the network. The UTN decides on the actions to be taken, and ensures that they are applied. It arbitrates disputes between its members.

The UTN may audit its members. The Certificates (Intermediate CAs or TSU) of UTN members may be revoked at any time, pursuant to the cases defined in this CP.

The UTN may delegate all or some of its functions.

1.2 Document name and identification

This document is the Timestamping Policy of the UTN.

This Timestamping Policy (TSP) is common to all Timestamping Authorities that are members of the UTN. It defines the commitments of the member TSAs of the network in terms of security and organisation of the processes for the issue and management of Timestamps issued by the member TSAs.

An OID is used for the Timestamps issued by the member TSAs of the UTN.

- The Timestamps, issued in compliance with [ETSI 319 421] and in accordance with this TSP, bear the OID 1.3.6.1.4.1.15819.5.2.2 or the OID 1.3.6.1.4.1.15819.5.2.3[1].

This policy is also compliant with the Timestamping Policy of the ETSI referenced by the OID 0.4.0.2023.1.1.

1.3 UTN participants

1.3.1 Certification Authorities

A Certification Authority (CA) refers to the authority in charge of creating, issuing, managing and revoking Certificates in pursuance of the Certification Policy.

Every member of the UTN defines one governing body for each CA: the Approval Board. It is empowered with the authorisations needed to:

- define and approve the Certification Practice Statement of the CA (CPS) in accordance with this CP;
- define the process for updating the CPS;
- inform the UTN about and provide it with the CPS and its revisions.

1.3.2 Registration Authorities

The Registration Authority (RA) is a component of the CA, in charge of identifying and authenticating Certificate applicants.

[1] These two types of Timestamps are recognised as qualified within the meaning of the eIDAS regulation (EU) No. 910/2014.

1.3.3 Subscribers

The Certificate Subscriber is the natural person or legal person who owns the Certificate. The Subscriber must have accepted the terms and conditions defined in the Subscriber Agreement.

1.3.4 Timestamping Authorities

A Timestamping Authority (TSA) refers to the authority in charge of creating and issuing Timestamps in accordance with the Timestamping Policy.

Every member of the UTN defines one governing body for each TSA: the Approval Board. It is empowered with the authorisations needed to:

- define and approve the certification practices of the TSA (TSPS) in accordance with this TSP;
- define the process for updating the TSPS;
- inform UTN about and provide it with the TSPS and its revisions.

The Certification Authorities issue Certificates for the Timestamping Units of the TSAs. These Certificates allow the Relying Parties to identify the TSA. The Certificates of TSUs are issued by a Timestamping CA of the UTN.

1.3.5 Relying parties

The Relying Parties are natural persons or legal persons who desire, for their own needs, to use the information contained in a Certificate or a Timestamp or to verify the validity of the Timestamp or Certificate. It is the duty of the Relying Parties to verify the information related to the revocation status of the Certificate.

The Relying Parties are subject to the stipulations of the Relying Party Agreement.

1.3.6 Certificate Officer

A Certificate Officer is a natural person who:

- carries out the tasks related to the life cycle of a Certificate of a legal person (from the Certificate application to its revocation);
- controls the use of the private key corresponding to this Certificate.

The Certificate Officer is appointed by the Certificate Subscriber. The Certificate Officer has a contractual, hierarchical or regulatory link with the legal person holding the Certificate and must be expressly mandated by it. The Certificate Officer must comply with the conditions stated in this CP, by the mandate that binds him to the Subscriber and by the Subscriber Agreement.

The Certificate Officer may need to be changed during the validity period of the Certificate (departure of the Certificate Officer from the entity, change of assignment and responsibilities in the entity, etc.). The Subscriber must immediately inform the CA about the departure or revocation of a Certificate Officer and appoint a new Certificate Officer. The CA must revoke a Certificate for which the Certificate Officer is no longer identified.

1.4 Certificate usage

1.4.1 Appropriate Certificate uses

Keypairs and Certificates of CAs The keypairs associated with the CA Certificates can be used to sign:

- the Certificates of Intermediate CAs (for Primary CAs);
- the Certificates of Subscribers (for Intermediate CAs);
- the CRL and/or OCSP responses of the CA;
- the Certificates of technical components of its infrastructure.

Keypairs and Certificates of Subscribers

The keypairs associated with the Certificates issued by the CA are intended to be used by the Subscribers for:

- signing documents with an electronic signature (for natural person Certificates issued by an Intermediate CA);
- sealing documents with an electronic seal (for legal person Certificates issued by an Intermediate CA);
- issuing Timestamps (for Certificates issued by a Timestamping CA).

1.4.2 Prohibited Certificate uses

Any use other than those specified in paragraph 1.4.1 is forbidden.

1.5 Policy administration

1.5.1 Organization administering the document

Universign Trust Network
Universign
7, rue du Faubourg Poissonnière, 75009 Paris, France

contact@universign.com

1.5.2 Contact person

Any questions related to this document may be addressed to:

The Policy Manager
Universign Trust Network
Universign
7, rue du Faubourg Poissonnière, 75009 Paris, France

contact@universign.com

1.5.3 Person determining TSP suitability for the policy

The UTN determines the appropriateness of a TSPS as regards the TSP.

1.5.4 TSPS approval procedures

The UTN pronounces the compliance of TSPS with the TSP according to an approval process that it defines at its discretion. This approval process includes audits conducted by UTN.

1.6 Definitions and acronyms

The terms used in this document are as follows:

Certificate Refers to the electronic file issued by the Certification Authority, comprising identification elements of its Subscriber and a cryptographic key allowing the verification of the Electronic Signature or Electronic Seal for which it is used.

Certification Authority (CA)
Refers to the authority in charge of creating, issuing, managing and revoking Certificates in pursuance of the Certification Policy.

Certification Policy (CP) Refers to all the rules that the CA must comply with for implementing the certification service.

Certification Practice Statement (CPS) Refers to the practices (organisation, operating procedures, technical and human resources) applied by the CA to implement its electronic certification service. These practices are compliant with the CP (s) that the CA has pledged to comply with.

Certificate Revocation List (CRL) Refers to the list identifying the Certificates issued and later revoked by the Certification Authority.

Object IDentifier (OID) Refers to the unique identification numbers organised hierarchically, which particularly enable referencing the conditions applicable to the certification or timestamping service, e.g. Certification or Timestamping Policy, Certificate family, Certification or Timestamping Practice Statements.

Online Certificate Status Protocol (OCSP) A protocol that allows the Relying Parties to verify the status of a Certificate.

Registration Authority (RA)
Refers to the authority in charge of implementing the identification and authentication procedures for Certificate applications.

Relying Party Agreement
Refers to the agreement governing the relations between UTN and the Relying Parties.

Subscriber Agreement
Refers to the agreement governing the relations between the CA and the Subscriber.

Timestamp Refers to the electronic file issued by the Timestamping Authority, which binds the representation of a piece of data to a particular time, thereby establishing proof that the data existed at the said moment.

Timestamping Authority (TSA) Refers to the authority in charge of creating and issuing Timestamps in pursuance of the Timestamping Policy.

Timestamping Policy (TSP) Refers to all the rules that the TSA must comply with for implementing the timestamping service.

Timestamping Practice Statement (TSPS) Refers to the practices (organisation, operating procedures, technical and human resources) applied by the

TSA to implement its timestamping service. These practices are compliant with the TSP (s) that the TSA has pledged to comply with.

Timestamping Unit (TSU) Set of hardware and software used by the TSA to create Timestamps. The TSU is identified via a unique key for sealing Timestamps.

2 Publication and repository responsibilities

2.1 Repositories

The TSA publishes information related to the service that it provides (see 2.2).

The UTN publishes the TSP in force and its prior versions as well as the Relying Party Agreement.

2.2 Published information

The TSA pledges to inform the Relying Parties about:

- la TSP applicable to the Timestamps that they use;
- the terms of use of the timestamping service;
- the TSPS related to the applicable TSP;
- the currently valid Certificates of the TSU.

The UTN provides the CA with a publishing website accessible at the address `http://docs.universign.eu` for providing the published information.

2.3 Time and frequency of publication

The time and frequency vary according to the information concerned:

- The TSU Certificates are distributed or uploaded before use.
- The TSP, TSPS and Relying Party Agreement are published after every update.

2.4 Access Controls on repositories

The published information is made public in accordance with section 2.1. They can be freely accessed in read-only mode.

Additions, deletions and modifications of this information are limited to only those persons who are authorised by the entity in charge of the published information.

3 Section left empty

4 Operational controls

4.1 Clock synchronisation

The TSA guarantees that its clock is synchronised with UTC time with a declared accuracy of one second.

More particularly:

1. the calibration of every TSU clock is maintained in such a way that the clocks cannot drift beyond the declared accuracy;

2. the clocks of the TSUs are protected from threats related to their environment, which could lead to a desynchronisation with the UTC time greater than the declared accuracy;

3. the TSA guarantees that the internal clock drift of a TSU beyond the declared accuracy will be detected.

4. if the clock of a TSU is detected as not being within the declared accuracy, Timestamps are no longer generated;

5. the TSA guarantees that the clock synchronisation is maintained when a leap second is scheduled, as notified by the appropriate body. The change to take into account the leap second is carried out during the last minute of the day on which the leap second is scheduled. A record is made of the exact time (as per the declared accuracy) when this change is made.

4.2 Mandatory algorithms

The TSA accepts the hashing algorithms compliant with the requirements of the authorities having jurisdiction in these matters. The accepted hashing algorithms are as follows:

- SHA-1[2]
- SHA-256
- SHA-384
- SHA-512

5 Facility, management, and operational controls

The TSA defines its Information Security Policy (ISP). It describes the approach and solutions to be implemented in terms of security management.

The ISP is kept up to date and approved by the TSA.

5.1 Physical controls

5.1.1 Site location and construction

The TSA hosts its services in secured premises. These sites and premises have physical security mechanisms that provide strong protection against unauthorised access.

5.1.2 Physical access

Access to the zones of the TSA services is restricted to only those persons who are authorised by name.

The premises consist of multiple successive physical security zones. Every successive zone offers a more restricted access with greater physical security against unauthorised access, due to the fact that each secure zone is encapsulated by the previous one.

[2] The use of this algorithm is still accepted for compatibility reasons. It is considered to be weak today. It is recommended to use one of the other algorithms from the list.

5.1.3 Power and air conditioning

Backup measures have been installed to ensure that any interruption in the power supply or a malfunctioning of the air-conditioning system does not harm the commitments made by the TSA in terms of availability.

5.1.4 Water exposures

The definition of the security perimeter takes water damage-related risks into account. Protective means are implemented by the host to mitigate the residual risks.

5.1.5 Fire prevention and protection

The secure zones are equipped with appropriate fire prevention and protection measures.

5.1.6 Media storage

The media are stored in a secure manner. The backup media are stored securely in a site that is geographically separate from the one storing the original media. Zones containing data media are protected from risks of fire, floods and deterioration. Paper documents are stored by the TSA in secure locked rooms, in a safe that can be opened only by the manager of the TSA and by authorised staff. The TSA takes measures to protect against the obsolescence and deterioration of the media during the records retention period.

5.1.7 Waste disposal

Media that is deemed sensitive in terms of confidentiality is destroyed, or may be reused in the operational context of an identical sensitivity level.

5.1.8 Off-site backup

In order to allow resumption of its commitments after an incident, the TSA makes off-site backups of its critical functions and information. The TSA guarantees that the backups are made by persons having Trusted Roles. The TSA guarantees that the backups are exported outside the production site and benefit from measures for protecting confidentiality and integrity. The TSA guarantees that the backups are regularly tested to ensure that the measures of the business continuity plan are followed.

5.2 Procedural controls

5.2.1 Trusted roles

The Trusted Roles defined in this chapter are applicable to all member TSA of the UTN.

The following Trusted Roles have been defined:

Security manager : he is fully responsible for all security aspects of the information system.

System Administration Manager : he is responsible for the system administrators. He possesses authentication rights on all components of the TSA.

System Administrator : he is in charge of the administration and configuration of all technical components of the TSA as well as for the day-to-day operating processes of the TSA. He is authorised to make backups and restores.

Auditor : he is authorised to audit the archives and all audit data of the TSA.

Controller : he is in charge of the recurring analysis of events occurring on the components of the TSA.

Secret Keeper : he ensures the confidentiality, integrity and availability of the secrets that are entrusted to him.

Staff occupying Trusted Roles must be free from any conflict of interest that is not compatible with their tasks.

5.2.2 Number of persons required per task

The TSA determines the procedures and number of persons having a Trusted Role that are needed for every action on sensitive operations.

5.2.3 Identification and authentication for each role

Identification and authentication measures have been defined in order to implement the access control policy and operations traceability. The assigned Trusted Roles are notified in writing to the persons concerned by the TSA. The TSA regularly ensures that all the Trusted Roles are filled in order to ensure business continuity.

5.2.4 Roles requiring separation of duties

The TSA ensures that the roles of Security Manager and System Administrator are not assigned to the same person.
The TSA ensures that the roles of Controller and System Administrator are not assigned to the same person.
The TSA ensures that the roles of Auditor and System Administrator are not assigned to the same person.
The TSA ensures that the security operations are separated from the conventional operating activities and that they are systematically conducted under the control of a person having a Trusted Role.

5.2.5 Risk analysis

The TSA carries out a risk analysis to identify the threats to its services. This risk analysis is reviewed periodically and during significant structural changes. Furthermore, the methodology used to carry out the risk analysis enables ensuring that the inventory of the TSA is kept up to date.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

The TSA ensures that the assignments of staff to Trusted Roles correspond to their professional skills. The supervisory staff possesses the appropriate expertise and is familiarised with the security procedures. Anyone intervening in Trusted Roles is informed of his responsibilities (job description) and the procedures related to system security and staff control. Staff occupying Trusted Roles are appointed by the management of the TSA.

5.3.2 Background check procedures

Before appointing a person to a Trusted Role, the TSA verifies his legal history and his professional skills, in order to validate his suitability to the job in question. The following details are especially verified:

- the person has no conflict of interest that would impact the impartiality of the tasks assigned to him;
- the person has not committed any offence that contradicts his Trusted Role.

The TSA selects persons for Trusted Roles in consideration of their loyalty, conscientiousness and integrity.

5.3.3 Training requirements

The staff is trained to operate the software, hardware and internal procedures in use.

5.3.4 Retraining frequency and requirements

Every change in the systems, procedures or organisations is covered by information or training for the intervening staff insofar as this change affects their work.

5.3.5 Job rotation frequency and sequence

Not applicable.

5.3.6 Sanctions for unauthorized actions

The sanctions in case of unauthorised actions are defined in contracts.
The nature of these sanctions is informed to the persons occupying a Trusted Role.

5.3.7 Independent contractor requirements

The requirements related to the staff of external service providers are formalised via contracts. The contracts signed with the service providers define the requirements related to confidentiality and security as well as the measures related to the use of computer resources.

5.3.8 Documentation supplied to personnel

The documented security rules and procedures are submitted to the Approval Board of the TSA for approval. The security rules are communicated to the staff at joining, depending on the role assigned to the intervening staff. The persons tasked with an operational role in the TSA have access to the corresponding procedures and are required to comply with them.

5.4 Audit logging procedures

5.4.1 Types of events recorded

The TSA takes the necessary measures to record the following events:

- the generation of Timestamps;
- all events related to the life cycle of the TSUs (context management, key management, certificate import, etc.);

- shut-downs/restarts of TSUs;
- the desynchronisation of the TSU clocks.

These logs enable ensuring the traceability and accountability of the actions conducted, especially in case of a request from a legal or administrative authority. In its internal procedures, the TSA describes the details of the recorded events and data. The traceability procedures implemented by the TSA are robust and help to aggregate logs from various sources, to detect intrusions and to develop a monitoring plan.

5.4.2 Frequency of processing log

The event logs are systematically used when an abnormal event is recorded.

5.4.3 Retention period for audit log

The event logs are stored for the duration required for providing evidence in administrative and legal proceedings.

5.4.4 Protection of audit log

The event logs are accessible only to authorised staff. They cannot be modified.

5.4.5 Audit log backup procedures

The logs are regularly backed up on an external system.

5.4.6 Audit collection system

The systems for collecting the event logs of the TSA are intended to be used to provide evidence during legal proceedings and in case of an administrative inspection. They also contribute to ensuring business continuity. The collected information is stored for an appropriate period of time, even after the discontinuation of the TSA 's business activities. They are relevant and proportional as regards their purpose.

5.4.7 Notification to event-causing subject

There is no notification of events.

5.4.8 Vulnerability assessments

The TSA implements controls for detecting:

- unauthorised access;
- technical anomalies;
- inconsistencies between different events of the TSA.

5.5 Records archival

5.5.1 Types of records archived

The following data is archived:

- the TSPS;
- the published CRLs and Certificates;
- the Subscribers ' registration data;
  - proof of acceptance of the general and special terms and conditions of use and/or the Subscriber Agreement (see Section **??**);
  - the Subscribers ' registration applications;
  - a copy of the information that enabled verifying the identify of a natural person;
  - the registration file of Subscribers (see section **??**);
- the event logs, particularly containing:
  - events related to a significant change in the TSA 's environment and the specific time of occurrence of the event;
  - events related to operations on the keys and certificates issued by the TSA and the specific time of occurrence of the event.
- the TSPS;
- the event logs, particularly containing:
  - events related to a significant change in the TSA 's environment and the specific time of occurrence of the event;
  - events related to operations on the keys of the TSUs and the specific time of occurrence of the event.

In its internal procedures, the TSA describes the details data and events that will be stored.

5.5.2 Retention period for archive

All the archives are preserved in compliance with the legislation in force (see Sect. 9.4.1)) and the obligation inherent to the TSA (see Sect. 5.8).

5.5.3 Protection of archive

Irrespective of their medium, the integrity of the archives is protected and they are accessible only to authorised persons. These archives can be consulted and used for the entire duration of their life cycle and are preserved in a secure environment.

5.5.4 Archive backup procedures

Regular electronic backups of the archives are made by persons having Trusted Roles. These backups are exported outside the production site and benefit from measures for protecting confidentiality and integrity.

5.5.5 Requirements for time-stamping of records

The event records must contain the date and time of the event. However, there is no requirement of a cryptographic timestamp for these events.

5.5.6 Archive collection system

The systems for collecting archives of the TSA are internal systems.

5.5.7 Procedures to obtain and verify archive information

The archives (hard and soft copies) can be recovered in a period of less than two working days. These archives are preserved and processed by teams of the TSA.

5.6 Key changeover

The TSA does not have an automatic key renewal procedure; instead, a TSA must generate new TSU keypairs and file Certificate applications with a Timestamping CA of the UTN before the end of the period of use of the private key of a TSU.

The TSA must apply all necessary actions to prevent any interruption of its operations.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

The TSA implements procedures and means for notifying and processing incidents. These means help to minimise damage in case of incidents.

The TSA implements a response plan in case of a major incident, such as the compromising of publishing mechanisms or its Certificate issuing mechanism.

A major incident, such as a loss, suspected compromising or theft of the private key of the TSU, is immediately notified to the Approval Board, which, if necessary, may decide to file a TSU Certificate revocation application with the UTN and to end the TSU.

5.7.2 Computing resources, software, and/or data are corrupted

A continuity plan has been implemented for responding to the availability requirements of the various components of the TSA. This plan is tested regularly.

5.7.3 Entity private key compromise procedures

This point is covered in the business recovery and continuity plans. If a TSU key becomes compromised, this immediately results in the revocation of its Certificat eand the shut-down of this TSU. In this case, the various persons and entities concerned are informed of the unsafe nature of the Timestamps signed by the compromised key of the TSU. Similar measures are taken if the soundness of the algorithm used or that of the parameters used by the TSU become insufficient.

5.7.4 Business continuity capabilities after a disaster

The business continuity capacity following a disaster is addressed in the business recovery and continuity plan. After a disaster, the TSA implements this plan in order to restore the affected services. In particular, the TSA has a redundant architecture for its critical services. Moreover, the TSA manages a stock of spare parts in order to handle any hardware breakdown.

In case of a major incident, the TSA has a business recovery plan that allows it to set up a new TSA within a reasonable period of time. This plan is based on a secondary host room.

Once its business is recovered, the TSA implements all necessary measures to prevent the recurrence of a similar disaster. The restoration operations are conducted by staff having Trusted Roles.

The Business Recovery Plan is tested regularly.

5.8 TSA termination

In case of a permanent shut-down, the TSA implements an end of life plan. This end of life plan addresses the following aspects:

- the notification of the shut-down to the persons and organisations affected by the plan;
- the notification of the shut-down to UTN;
- the potential revocation of all issued Certificates that are still valid when the decision was made to discontinue the business activity;
- the destruction of the private keys of the TSUs;
- the measures required to transfer its obligations related to the archives of audit data;
- the provision of information for Relying Parties.

This plan is verified and updated regularly.

6 Technical security controls

6.1 Keypair generation and installation

6.1.1 Keypair generation

The keys of the TSU are generated:

- during a key ceremony in front of witnesses;
- under the control of at least two persons having Trusted Roles (see Sect. 5.2.1);
- in secure premises (see Sect. 5.1);
- in an HSM compliant with the requirements defined in section 6.2.11.

The keys are generated according to a specific procedure and result in the drafting of a report after the ceremony.

The public keys of the TSUs are transmitted to the CA in accordance with the CP of the UTN.

6.1.2 Private key delivery to Subscriber

Not applicable.

6.1.3 Public key delivery to CA

The public key to be certified is transmitted to the CA in order to guarantee the integrity and source of this key.

6.1.4 CA public key delivery to Relying Parties

Not applicable.

6.1.5 Key sizes

The TSU keys must be compliant with (or cryptographically superior or equal to) the following characteristics. They must also be compliant with the requirements of the CP of UTN.

Certificate	Key Size	Format
TSU	2048 4096 (for keys generated after 1 January 2019)	RSA RSA

6.1.6 Public key parameters generation and quality checking

The TSAs must use certified hardware (see Sect. 6.2.11)) and algorithms whose parameters comply with the appropriate security standards.

6.1.7 Key usage purposes

See section 7.1.

6.2 Private key protection and cryptographic module engineering controls

6.2.1 Cryptographic module standards and controls

The cryptographic modules used by the TSA for generating and implementing its signature keys are certified hardware cryptographic modules that comply with the requirements of section 6.2.11. The TSA ensures the security of these modules throughout their life cycle. In particular, the TSA implements the procedures required for:

- ensuring their integrity during their transport from the supplier;

- ensuring their integrity during their storage before the key ceremony;
- ensuring that the operations of activation of the signature keys are conducted under the control of two staff members having Trusted Roles;
- ensuring that they are in a proper functional state;
- ensuring that the keys that they contain are destroyed after being decommissioned.

6.2.2 Private key (n out of m) multi-person control

The private key of a TSU is controlled by the activation data stored on the smart cards handed over to the secret keepers during the key ceremony. A sharing of the HSM's secret is implemented by the TSA.

6.2.3 Private key escrow

The private keys are not escrowed.

6.2.4 Private key backup

No backup copies are made of the private keys of TSUs.

6.2.5 Private key archival

The private keys of the TSA are not archived.

6.2.6 Private key transfer into or from a cryptographic module

Not applicable.

6.2.7 Private key storage on cryptographic module

The private keys of the TSUs are stored in a cryptographic module.

6.2.8 Method to activate the private key

The activation of private keys is controlled by specific data referred to as activation data. It is carried out in a cryptographic module that complies with the requirements of section 6.2.11, under the control of two persons with Trusted Roles.

6.2.9 Method to deactivate the private key

The private key is deactivated when the cryptographic module is shut down.

6.2.10 Method to destroy the private key

The private key of a TSU is destroyed from its cryptographic module. The TSA ensures that all corresponding backup copies are also destroyed.

6.2.11 Cryptographic Module Rating

Cryptographic module of TSUs: The cryptographic modules of TSUs comply with the following certification requirements:

- EAL 4+ as regards the Common Criteria of ISO/CEI 15408 (compliant with Protection Profile CWA 14169 or certified as compliant with the Protection Profile of a Secure Signature Creation Device (SSCD) by a European governmental entity);
- FIPS 140-2 level 3
- QSealCD within the meaning of regulation eIDAS (EU) No 910/2014.
- or equivalent.

6.3 Other aspects of key pair management

6.3.1 Public key archival

The TSA archives the public keys of its TSUs as per the requirements of section 5.5.

6.3.2 Certificate operational periods and key pair usage periods

The maximum service life of the Certificates is:

- 30 years for the Primary CA Certificates;
- 20 years for the Timestamping CA Certificates;
- 15 years for the Intermediate CA Certificates;
- 5 years for natural person Certificates and legal person Certificates;
- 11 years for legal person Certificates intended for timestamping.

6.4 Activation data

6.4.1 Activation data generation and installation

The activation data of a TSU's key is generated during the key ceremony. This activation data is stored on smart cards and handed over to the secret keepers.

Every secret keeper takes the necessary measures to protect themself against the loss, theft, unauthorised use or unauthorised destruction of their smart card and the activation data that it contains.

6.4.2 Activation data protection

The activation data is stored on a nominative and personal smart card. The responsibility for this smart card falls on the person to whom the card is submitted. The card is protected by a personal password of the secret keeper. The smart cards are then stored in a personal secure safe. Every secret keeper is responsible for their part of the activation secret. They give their consent by signing a form defining their responsibilities.

6.4.3 Other aspects of activation data

Transmission of activation data: The transmission of smart cards containing activation data from one secret keeper to a new secret keeper must be carried out in such a way as to protect the activation data from loss, theft, modification, unauthorised disclosure or unauthorised use of this data.

Destruction of activation data: The activation data is decommissioned in order to prevent the theft, loss, modification, unauthorised disclosure or unauthorised use of this data.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

Depending on the system to be protected, the TSA implements control mechanisms that are appropriate as regards the platform to be secured (in order to protect against the execution of an unauthorised or potentially dangerous code on its system).

The TSA implements access control and authentication mechanisms for all roles authorised to generate new certificates. It maintains these security systems continuously. These mechanisms are described in the TSPS.

6.5.2 Computer security rating

Not applicable.

6.6 Life cycle technical controls

6.6.1 System development controls

All software components of the TSA are developed under conditions and according to development processes that guarantee their security. The TSA implements quality processes during the design and development of its software.

When beginning production of a software component, the TSA checks its source and its integrity and ensures a traceability of all modifications made to its information system.

The development and testing infrastructure are separate from the production infrastructure of the TSA.

6.6.2 Security management controls

The TSA ensures that the software programs are updated in such a way as to ensure system security. The updates are carried out by persons having a Trusted Role in the TSA.

6.6.3 Life cycle security controls

Not applicable.

6.7 Network security controls

Network communications containing confidential information are subjected to protective measures against eavesdropping. The rules governing these controls are verified regularly.

Security measures are implemented in order to protect the local components of the information system from unauthorised access, especially for sensitive data.

The TSA implements platform administration access management procedures in order to maintain a high level of security. These measures include the authentication of administrators, the production of logs for audits, the use of secure VPN-type channels as well as the possibility of modifying access rights at any time. The CA also implements an administration network that is disconnected from the nominal network.

The TSA implements access control procedures to separate the administration functions and the operational functions. The use of applications (publishing, certificate generation, revocation) requires an authentication of the users or entities. An access control policy is implemented to limit access to these applications to authorised persons only.

6.8 Time accuray

The TSU clocks are supervised locally by the reference time servers. These servers are autonomous and benefit from a synchronisation procedure with the UTC(k) references. The mechanisms used enable protecting against attacks aiming to desynchronise the time systems, including major attacks that aim to scramble radio or satellite signals.

The TSA guarantees that the Timestamps generated by its TSUs have a time drift of less than one second with respect to the UTC.

7 Profil of TSU Certificates and Timestamps

7.1 Profile of TSU Certificates

The profile of TSU Certificates is defined in the CP of UTN.

7.2 Profile of Timestamps

version	Version 1
policy	OID : 1.3.6.1.4.1.15819.5.2.(2/3)
messageImprint	OID of the hashing algorithm and digital imprint data to be timestamped. Note: This information is provided in the request.
serialNumber	Random 160-bit number characterising this request.
genTime	Timestamping date in the ASN.1 GeneralizedTime format.
accuracy	Accuracy of 1 second
ordering	Content set to FALSE
nonce	Value resent without any change if present in the request.
tsa	The name of the TSU
extensions	Not applicable..

8 Compliance audit and other assessments

8.1 Frequency or circumstances of assessment

Audits are conducted by the TSA:

- an internal audit conducted
- either by external service providers specialising in the domain;
- or by an internal lead auditor of the TSA.
- a certification audit for standards [ETSI 319 411-1] and [ETSI 319 411-2], conducted every 2 years by an accredited body.

A control of compliance with the TSPS in force is conducted:

- during the operational implementation of the system;
- at least once per calendar year (internal audit);
- during the surveillance or renewal of certifications, in accordance with the regulatory procedures in force;
- when a significant change is carried out.

8.2 Identity/qualifications of assessor

The evaluators must ensure that the policies, statements and services are correctly implemented by the TSA and detect cases of non-compliance that could compromise the security of the offered service. The TSA pledges to appoint evaluators whose skills are proven in matters of information system security and who are specialised in the domain of activity of the controlled component.

8.3 Assessor's relationship to assessed entity

Unless specifically agreed between the TSA and the UTN, the TSA appoints the evaluator authorised to conduct the audit. The TSA guarantees the independence and impartiality of the evaluator.

8.4 Topics covered by assessment

The evaluator checks the compliance of the audited component, on all or part of the implementation of:

- the TSP;
- the TSPS;
- the components of the TSA.

Before every audit, the evaluators suggest a list of components and procedures that they wish to verify to the Approvals Committee of the TSA. They use this to develop the detailed audit plan.

8.5 Actions taken as a result of deficiency

After a compliance check, the evaluator and his team submit a verdict to the Approvals Committee of the TSA, which can be: “successful”, “failed”, “to be confirmed”.

“Failed” verdict: The audit team issues recommendations to the TSA. The TSA can choose the measures to be applied.

“To be confirmed” verdict: the audit team identifies the non-compliances and ranks them. The TSA should then suggest a schedule for resolving the non-compliances. A verification will be used to ensure that the identified non-compliances have been resolved.

“Successful” verdict: the TSA confirms that the controlled component is compliant with the commitments of the TSP and its announced practices.

8.6 Communication of results

The results of the compliance audits are sent to the Approval Board, to the UTN and are made available to the authorities in charge of qualifying and certifying the service.

9 Other business and legal matters

9.1 Fees

The members of UTN determine the pricing conditions of their services.

9.1.1 Fees for other services

No specific commitment.

9.1.2 Refund policy

The TSA services are not subject to any reimbursement.

9.2 Financial responsibility

9.2.1 Insurance coverage

The members of the UTN subscribe to an appropriate liability insurance that covers the financial risks related to the use of the service that it provides, in accordance with the regulations applicable to its business.

It is the duty of the TSA to evaluate the financial risk that is to be covered.

9.2.2 Other assets

The TSA implements an administrative and financial policy that aims to maintain, throughout the duration of its business, the financial resources required for fulfilling the obligations defined by the TSP.

9.2.3 Insurance or warranty coverage for end-entities

No specific commitment.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

The following information is considered to be confidential:

- the private keys of the TSA,
- the activation data associated with the private keys of the TSA,
- the event logs,
- the audit reports,
- the business continuity, recovery and stoppage plans.

Other information may be considered as confidential by the TSA.

9.3.2 Information not within the scope of confidential information

The publishing website of the TSA and its contents are deemed as public.

9.3.3 Responsibility to protect confidential information

The TSA pledges to process confidential information in accordance with the obligations applicable to it.

9.4 Privacy of personal information

9.4.1 Privacy policy

The TSA collects and processes personal data in accordance with the regulations related to personal data protection that are applicable to it.

9.4.2 Personal information

Not applicable.

9.4.3 Non-personal information

Agreements between the TSA and the users of its services may comprise a special processing of non-personal and non-confidential information, within the meaning of article 9.3.1.

9.4.4 Responsibility to protect personal

The TSA is responsible for processing the personal data of the users of its service.

9.4.5 Notice and consent to use personal information

The TSA informs the persons, about whom it collects personal data, about the processing of this data and the purposes of this processing.

9.4.6 Disclosure pursuant to judicial or administrative process

Not applicable.

9.4.7 Other information disclosure circumstances

Agreements between the TSA and the users of its services may provide for the disclosure of personal information within the limits defined by French regulations.

9.5 Intellectual property rights

As part of its business activity, the CA may be required to issue or permit the use of elements protected by intellectual or industrial property rights.

These elements and the associated copyrights shall remain the property of the owner of these rights. The Relying Parties may reproduce these elements for their internal use. Prior authorisation of the copyright holder is required for the provision to third parties, extraction or reuse in whole or in part of these elements or of their derivative works or copies, aside from the requirements of the TSA 's service.

Any use or reproduction, in whole or in part, of these elements and/or the information that they contain, not authorised by the other party and used for any purpose other than the operation of the service, is strictly forbidden and constitutes infringement, which may be penalised through legal proceedings.

The use of the information contained in the Timestamps or related to their status is authorised in strict compliance with the Relying Party Agreement.

9.6 Representations and warranties

The common obligations of the TSA of UTN are as follows:

- to protect and guarantee the integrity and confidentiality of their private cryptographic keys;
- to use their private cryptographic keys only pursuant to the conditions of and with the tools specified in the TSP;
- to apply and comply with the requirements of the TSP and the TSPS applicable to them;
- to submit to the compliance audits conducted by the audit team mandated by UTN;
- to accept the consequences of these audits and in particular, to remedy any non-compliances that may be reported;
- to document their internal operating processes;
- to implement the (technical and human) resources needed for executing the operations that they are in charge of, while guaranteeing the quality and security of these operations.

9.6.1 Timestamping Authoriry

The TSA is responsible for:

- the compliance of the TSPS vis-à-vis the TSP;
- the compliance of the Timestamps with the TSP;
- the compliance of all different components of the TSA and the related controls with the principles of security.

The TSA is responsible for the damages caused to Relying Parties if the date and time indicated by the Timestamp and the integrity of the data that this date and time relate to are erroneous.

9.6.2 RA service

See above.

9.6.3 Subscriber

The Subscriber:

- communicates accurate and up-to-date information when filing an application for a Certificate;
- is responsible for access to its private key and, if applicable, the activation means of its key;
- complies with the conditions for use of its private key;
- informs the CA of any change in the information contained in its Certificate;
- immediately sends a Certificate revocation application if there is any suspicion of the corresponding private key or the activation means of this key becoming compromised.

9.6.4 Relying Parties

The Relying Parties pledge to comply with the obligations defined in the Relying Party Agreement and to familiarise themselves with the terms and conditions of the TSP applicable to the service that they use, particularly the limits of use and guarantees associated with the service

9.6.5 Other participants

No specific commitment.

9.7 Disclaimers of warranties

The limits of guarantee of the TSA are defined in the conditions of use of the timestamping service and the Relying Party Agreement.

9.8 Limitations of liability

The TSA cannot be held liable in case of any use of the Timestamps that is unauthorised or does not comply with the TSP, the Subscriber Agreement or the Relying Party Agreement.

The TSA cannot be held liable for indirect damages resulting from the use of a Timestamp.

The TSA is not responsible for any use that is unauthorised or non-compliant with the documentation of their equipment and/or software provided to the users of the timestamping service.

9.9 Indemnities

The conditions for compensation of damages caused to Subscribers and to Relying Parties are defined contractually.

9.10 Term and termination

9.10.1 Term

The TSP comes into force once it is published on the publishing website of UTN.

9.10.2 Termination

The TSP remains valid until it is replaced by a new version.

9.10.3 Effect of termination and survival

Unless specified otherwise in this TSP or in the TSP that will replace it, the end of validity of the TSP results in the nullity of all obligations of the TSA applicable to the Timestamps issued in accordance hereof.

9.11 Individual notices and communications with participants

Unless agreed otherwise by the parties concerned, all individual notifications and communications mentioned in the TSP must be sent by means that guarantee their origin and their receipt.

9.12 Amendments

9.12.1 Procedure for amendment

The UTN may amend the TSP. These amendments take the form of new versions of the TSP. They are published on the publishing website of the UTN. The UTN determines whether the changes to the TSP require a change in the OIDs for the issued Timestamps.

9.12.2 Notification mechanism and period

The UTN may make unannounced changes to the TSP in force in case of a minor change, such as spelling or URL errors. The UTN is the sole entity authorised to assess whether a change is minor or not.

The UTN informs its members about its intent to modify the TSP, by specifying the suggested modifications and the commenting period. These change proposals are also published on the website of the UTN. Members who administer their own publishing website must publish the change proposals on it as soon as they are received.

Commenting period: Unless specified otherwise, the commenting period is one (1) month from the publishing of the proposal for non-minor changes on the publishing website of the UTN. All entities intervening in the UTN may submit comments during this period.

Processing of comments: Once the commenting period ends, the UTN may decide to publish the new TSP or once again initiate a new amendment process with a modified version or withdraw the proposed version.

9.12.3 Circumstances under which OID must be changed

If there is a substantial change in the TSP, the Approval Board of UTN may decide that a change in OID is necessary

The OID may be changed if the modification of the TSP is likely to affect the assurance level of already issued Timestamps.

9.13 Dispute resolution provisions

The TSA implements an adequate procedure for amicably settling disputes between it and the users of its services.

9.14 Governing law

In the case of a dispute between the TSA and the UTN arising from the interpretation, application and/or execution of the TSP and if no amicable settlement can be reached by the parties as described above, exclusive jurisdiction is granted to the courts under the Court of Appeal of Paris.

9.15 Compliance with applicable law

The provisions of the TSP are compliant with the applicable requirements of French law.

The legislative and regulatory texts applicable to the TSP are, mainly, those indicated in the references of this policy.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

The TSA may specify specific requirements in the TSPS.

9.16.2 Assignment

No specific commitment.

9.16.3 Severability

If a clause of the TSP becomes null or is deemed unwritten by the verdict of a court having jurisdiction, the validity, legality and enforceable nature of the other clauses shall not be affected or reduced in any manner whatsoever.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

The requirements defined in the TSP must be applied in accordance with the provisions of the TSP and the associated TSPS and no exemption of rights, with the intent to modify any prescribed right or obligation, shall be possible.

9.16.5 Force majeure

The TSA shall not be held liable for indirect damages and the interruption of its services resulting from force majeure, which caused direct damage to their users.

9.17 Other provisions

9.17.1 Organization reliability

To guarantee the impartiality of its services, the TSA ensures that the persons occupying Trusted Roles do not suffer from any conflicts of interest that would harm the impartiality of their tasks.

9.17.2 Accessibility

Insofar as possible, the TSA allows disabled persons to access the services that it provides.

References

[**RFC 3647**]
Network Working Group - Request for Comments: 3647 - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework - November 2003.

[**ETSI 319 401**]
ETSI EN 319 401 V2.1.1 - Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers (2016-02)

[**ETSI 319 411-1**]
ETSI EN 319 411-1 V1.1.1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements (2016-02)

[**ETSI 319 411-2**]
ETSI EN 319 411-2 V2.1.1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates (2016-02)

[**ETSI 319 412-2**]
ETSI EN 319 412-2 V2.1.1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons (2016-02)

[**ETSI 319 412-3**]
ETSI EN 319 412-3 V1.1.1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons (2016-02)

[**ETSI 319 412-5**]
ETSI EN 319 412-5 V2.1.1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QC Statements (2016-02)

[**ETSI 319 421**]
ETSI EN 319 421 V1.1.1 - Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps (2016-03)