Time-Stamping Policy

Universign

Universign
OID: 1.3.6.1.4.1.15819.5.2.2
Version: 1.4
PUBLIC DISTRIBUTION

Contents

1 Introduction

1.1 Overview

UNIVERSIGN, being both a Time-Stamping Authority (TSA) and a Time-Stamping Service Provider (TSSP), offers to its customers a Time-Stamping Service (TSS) complying notably with the qualification requirements of the "Référentiel Général de Sécurité" (RGS) for a TSS.

The document herein is the UNIVERSIGN Time-Stamping Policy (TSP). It describes the UNIVERSIGN TSS and specifies the commitments of UNIVERSIGN as a TSA towards this very service. The present TSP also describes obligations and requirements of Subscribers and Relying Parties.

A Time-Stamp Token (TST) generated by UNIVERSIGN TSS provides evidence of the existence of a hash value at a given date and time. The TSTs are generated and digitally signed by the TSA through the use of Time-Stamping Units (TSUs).

This document aims at specifying UNIVERSIGN commitments when, acting as TSA, it delivers and manages TSTs, as well as the obligations of other participants.

This document comes with, for its implementation part, a Time-Stamping Practice Statement (TSPS) and the TSS Terms of Use (ToU). UNIVERSIGN TSPS presents the mechanisms and procedures implemented in order to reach the TSP security target, and in particular the process to be followed by a TSU when generating TSTs and maintaining the accuracy of its clocks. UNIVERSIGN acting as TSA may setup several TSUs in order to manage its TSS.

The Certification Authority (CA) delivering the certificates for the TSUs of the TSA also belongs to UNIVERSIGN. Its specifications are described in the Certification Policy (CP) of UNIVERSIGN CA: [**UCP**].

This TSP does not require any link between the hash to be time-stamped and the contents of the original electronic data. Only the Subscriber of the TSS is responsible for this match.

Within this TSP, day and time of each TST are synchonized with the Coordinated Universal Time (UTC) with an accuracy of less than one second. This TSP applies the standard TST format specified in the [**RFC 3161**] document. Sec-

tion 6.1 specifies the management of the TSS clock synchronization.

This TSP is based on the following documents: the ETSI TS 102 023 standard [**ETSI TSP**] and the standard TSP defined by the French RGS [**RGS_A_12**].

Principle of UNIVERSIGN TSS

Time-Stamping establishes evidence that a datum exists at a particular time. For this matter, it binds an unequivocal representation of a datum (i.e.: its hash value together with an hash algorithm identifier) to a particular time. A TST unequivocally performs this link; a TST is a signed structure including notably:

- the hash value and the hash algorithm of the time-stamped datum;
- date and universal time (UTC);
- the identifier of the TSU certificate that has generated the TST;
- the identifier of UNIVERSIGN acting as TSA (within the time-stamp certificate);
- the identifier of the CA that has signed the private keys installed on the TSUs.

UNIVERSIGN TSS benefits from the Public Key Infrastructure (PKI) that has been established by UNIVERSIGN, including the certification service of UNIVERSIGN CA.

This certification service allows UNIVERSIGN CA to issue the certificates of UNIVERSIGN TSUs.

The clock synchronization system of the TSS allows UNIVERSIGN to ensure the Subscriber the delivery of a TST with an accuracy of less than one second with respect to UTC.

UNIVERSIGN TSA operates several TSUs. Each TSU signs TSTs on behalf of the TSA, using a dedicated private key, which matching public key has been previously certified by UNIVERSIGN CA. Therefore each TSU has its own time-stamping certificate.

1.2 Document identification

This document is UNIVERSIGN Time-Stamping Policy. This TSP is identified, within the documentation framework of UNIVERSIGN trust architecture, by a unique identification number: **1.3.6.1.4.1.15819.5.2.2**

This OID is built as follows:

1.3.6.1.4.1.15819	CRYPTOLOG branch (registered with ETSI)
1.3.6.1.4.1.15819.5	Policies branch
1.3.6.1.4.1.15819.5.2	Time-Stamping policies branch

TSTs abiding by this policy refer to it by using this unique identifier (OID). Its value is included in the "Policy" field of the TSTs. Other more meaningful elements (name, version number, date of update) can also identify it.

1.3 TSS participants

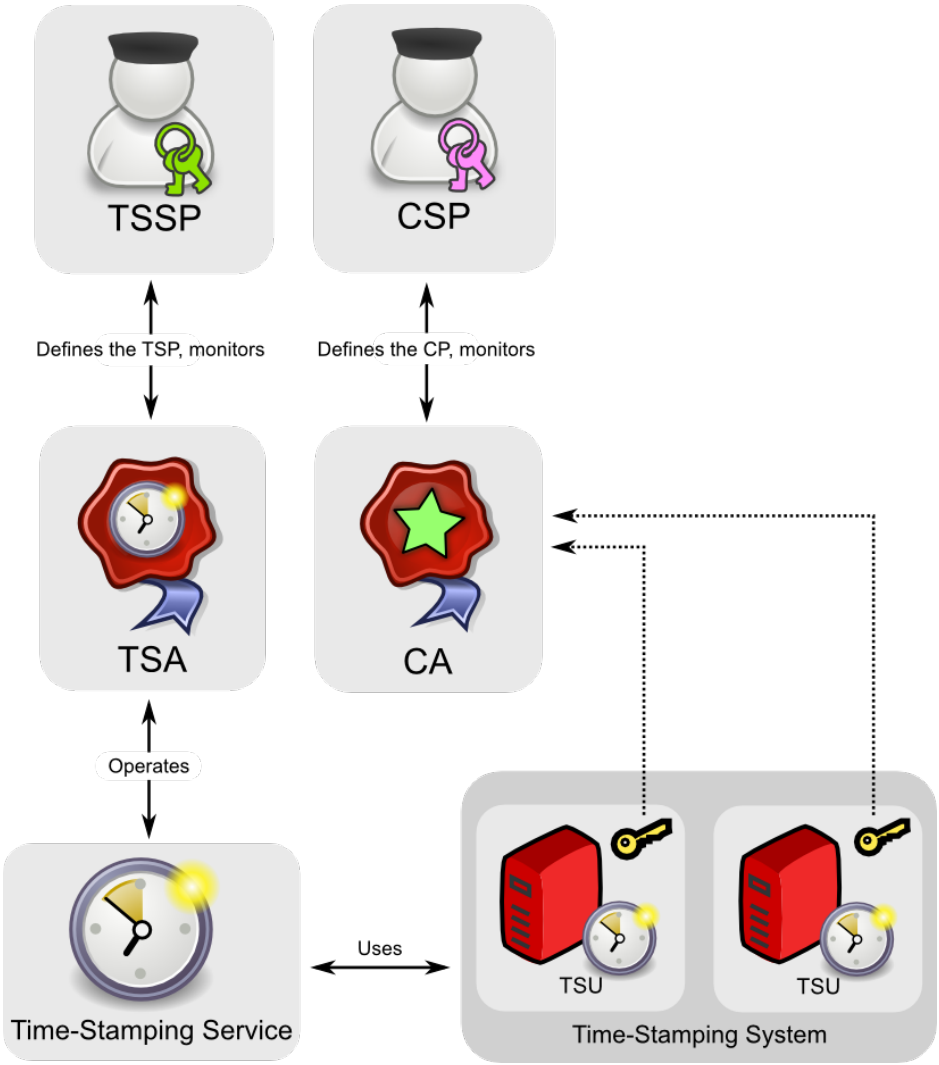

Figure 1: UNIVERSIGN TSS organization

1.3.1 Certification Authorities

Within a TSS, the TSU certificates are supplied by a CA. These certificates allow Relying Parties to identify the TSA.

1.3.2 Time-Stamping Authorities

In the French regulatory context, a Time-Stamping Authority and a Time-Stamping Service Provider are two notions that comes naturally together.

The "ordonnance" 2005-1516 [**ORD**] introduces and defines trust service providers (in French *Prestataire de Services de Confiance – PSCO*). A TSSP is a specific kind of PSCO. A TSSP is defined as a person or an entity responsible for the generation of the management of TSTs, with respect to its Subscribers and Relying Parties. A TSSP includes at least one TSA, but could have several depending on its organization. A TSSP is identified in the certificates of the TSU which it is responsible for through its TSAs.

Within a TSSP, a TSA is in charge, in name of and under the responsibility of the TSSP, of the application of at least one TSP, by using one or more TSUs. In the scope of this TSP, the term TSSP is not used outside this section and section 1.1 and only the term TSA is used. It designates the UNIVERSIGN TSA in charge af applying this TSP, within the UNIVERSIGN TSSP.

The TSA is managed by the Approval Board of UNIVERSIGN. UNIVERSIGN executive management sits in the Approval Board. The TSA Chief Officer is the chairman of this board.

The board approves the TSP and the documents regarding the TSS provided by UNIVERSIGN.

The board has the final authority and responsibility for:

- specifying and approving the infrastructure and practices of the UNIVERSIGN TSS;
- approving the UNIVERSIGN TSPS and TSP;
- ensuring the perennity of the TSPS and the TSP stated by the TSA in the scope of functional, organizational and technical requirements;
- ensuring the perennity of the compliance of the TSU implementation with the TSPS;
- publishing the TSP and the ToU and their revisions to Subscribers and Relying Parties.

1.3.3 Subscribers

A Subscriber is an entity requiring the services provided by UNIVERSIGN and which has agreed to its ToU.

1.3.4 Relying Parties

A Relying Party is an individual or entity that acts in reliance of a TST generated under this policy by the UNIVERSIGN TSA. A Relying Party may, or may not also be a Subscriber.

1.3.5 Other Participants

Not applicable.

1.4 Policy administration

1.4.1 Organization administering the document

UNIVERSIGN
Cryptolog International
6-8, rue Basfroi, F-75011 Paris, France
contact@universign.eu

1.4.2 Contact person

Questions concerning this TSP should be sent to:

The Time-Stamping Policy Manager
UNIVERSIGN
Cryptolog International
6-8, rue Basfroi, F-75011 Paris, France
contact@universign.eu

1.4.3 Person determining TSP suitability for the policy

The UNIVERSIGN Approval Board determines the suitability and applicability of this TSP.

1.4.4 TSP approval procedures

The approval of the conformance of the documented practices with the CP is pronounced by UNIVERSIGN Approval Board, in the light of the internal audits performed.

1.5 Definitions and Acronyms

Definitions

Auditor:
Person auditing the events of the TSS.

Certificate Revocation List (CRL):
The Certificate Revocation List is a list, digitally signed by the CA, and containing all the identifiers of the certificates that have been revoked prior to their expiration date.

Hash value:
Result of a hash function which characterizes a datum; it is a bit string with a fixed length for a specific hash function (for example 256 bits for SHA-256).

Hosting Provider:
Entity which hosts the technical platform of the service in a secure environment and a high availability network acccess.

Partners:
UNIVERSIGN defines a partner as a person, a group, a community or an entity with which UNIVERSIGN partners in order to provide its TSS to Subscribers and Relying Parties.

Time-Stamping Service (TSS):
Set of operations necessary to perform generation and management of TSTs.

Time-Stamping System:
Set consisting of all the TSUs together with the administration and supervision components used in order to provide the TSS.

Time-Stamp Token (TST):
Data object that binds a representation of a datum to a particular time, expressed in universal time (UTC), thus establishing evidence that the datum existed at that time.

Time-Stamping Unit (TSU):
Set of hardware and software used to create TSTs, characterized by an identifier of the Time-Stamping Unit certified by a CA, and which has a single TST signing key.

Universign:
In the scope of this document and the documents ruling the Time-Stamping offer, the Cryptolog International Company, SAS with a capital of 504 932 euros, 6-8, rue Basfroi, F-75011 Paris, registered with the Paris Registry of Companies under the number 439129164.

Acronyms

CA: Certification Authority

CNIL: Commission Nationale de l'Informatique et des Libertés (French board enforcing law on data protection)

CRL: Certificate Revocation List

NTP: Network Time Protocol

OID: Object IDentifier

RGS: Référentiel Général de Sécurité (Set of documents published by the French government, and regulating IT security within public administrations)

ToU: Terms of Use

TSA: Time-Stamping Authority

TSP: Time-Stamping Policy

TSPS: Time-Stamping Practice Statement

TSS: Time-Stamping Service

TSSP: Time-Stamping Service Provider

TST: Time-Stamp Token

TSU: Time-Stamping Unit

2 Publication and repository responsibilities

2.1 Repositories

UNIVERSIGN, as a TSA, provides Relying Parties with this TSP. This TSP is available on Internet, on the web site: http://docs.universign.eu.

Informations related to TSPS meant to be publicly distributed are included in this TSP and the ToU.

2.2 Publication of information

The published informations are the following:

- this TSP;
- the corresponding ToU;
- the certificates of the TSUs.

2.3 Time or frequency of publication

A new TSP will be published when:

- substancial modifications of the TSPS have an impact on this TSP;
- regulatory evolutions have an impact on this TSP;

The TSU certificates are published at most 24 hours after their generation and necessarily prior to their effective use.

2.4 Access controls on repositories

The published informations are published on the UNIVERSIGN web site and can be freely read by anyone. The TSP and the ToU are freely readable by anyone wishing to access them on the UNIVERSIGN web site: http://docs.universign.eu.

Additions, removal and modifications of these informations are limited to authorized UNIVERSIGN personnel, through access control.

3 General provisions

3.1 TSA obligations

UNIVERSIGN must comply with the requirements and the procedures defined in this TSP.

UNIVERSIGN must comply with any additional obligations indicated in the TST either directly or incorporated by reference.

UNIVERSIGN must supply a TSS in accordance with its TSPS.

UNIVERSIGN must fulfill all its commitments in compliance with its ToU.

UNIVERSIGN must ensure the technical issuance of the TSTs.

UNIVERSIGN must ensure that its TSPS is applied and that the requirements specified in the present TSP are satisfied.

3.2 Subscriber obligations

The Subscriber must accept and abide by the ToU of the UNIVERSIGN TSS.

The Subscriber should also verify that the certificate of the TSU which delivers a TST is valid when the time-stamp request is performed (see chapter 6.8).

3.3 Relying Party obligations

The Relying Party must verify that the CTs have been correctly signed and that the corresponding TSU certificate is not revoked at the time of verification, by using the CRLs published by the UNIVERSIGN CA.

The Relying Party must also verify that the TSTs requests are actually issued by an UNIVERSIGN TSU. To do so, the Relying Party must verify that the TST includes a reference to an UNIVERSIGN TSU.

Finally, the Relying Party should take into account the TST use limitations described in this TSP and the related ToU.

3.4 Obligations for the CAs providing the TSU certificates

The TSU certificates must be issued by a CA which has been qualified according to the French RGS for the "Cachet" Certificate Policy at the level at least one star (*).

3.5 TSPS

UNIVERSIGN ensures that it has the reliablity needed to provide a TSS and describes within its TSPS how this TSS is implemented. This document warrants that:

1. UNIVERSIGN carries out a risk assessment in order to evaluate business assets and threats to those assets in order to determine the necessary controls and operational procedures;
2. UNIVERSIGN has a statement of the practices and procedures used to address all the requirements identified in the present TSP;
3. The TSPS identifies the obligations and the implementation requirements to be complied with by the TSA, the Partners, the Subscribers and the Relying Party, in the scope of UNIVERSIGN TSS;
4. UNIVERSIGN provides Subscribers and Relying Parties with the public part of its TSPS (by including it in its ToU), so that they can assess conformance to this TSP.
5. UNIVERSIGN implements a relevant organization for the approval of its TSPS and the verification of conformity between this statement and this TSP;
6. The TSA Chief Officer ensures that the practices are properly implemented;
7. UNIVERSIGN defines a periodic control procedure in order to verify that its practices comply with its TSPS;
8. UNIVERSIGN aims at a certification of compliance with the present TSP delivered by an independent certification body.

Subsequently, any amendment initated by UNIVERSIGN and which could affect the compliance with its TSP or its TSPS will again be submitted to the opinion of an independent certification body.

Note: The TSPS is not intended to be publicly distributed. A formal request to UNIVERSIGN TSA is needed in order to get access to it.

3.6 ToU

UNIVERSIGN provides its ToU to its Subscribers. Subscribers must respect the clauses contained in these ToU.

These ToU are public and are published on UNIVERSIGN web site at: http://docs.universign.eu.

3.7 Conformance with legal requirements

3.7.1 Applicable law

The present document is governed by French law.

3.7.2 Litigation settlement

IN CASE OF LITIGATION BETWEEN THE PARTIES RESULTING FROM THE INTERPRETATION, THE APPLICATION AND/OR THE EXECUTION OF THE CONTRACT, AND IN THE ABSENCE OF MUTUAL AGREEMENT BETWEEN THE AFOREMENTIONNED PARTIES, THE ONLY COMPETENT JURISDICTION IS THE PARIS TRIBUNAL OF COMMERCE.

3.7.3 Intellectual property of UNIVERSIGN infrastructures

Regarding intellectual property, the products operated to provide the TSS belong to UNIVERSIGN.

The Subscribers or Relying Parties of these services have no intellectual property rights to these various elements. Any use or reproduction, total or partial, of these elements and / or information within, by any means, is strictly prohibited and is a forgery punished by the ”Intellectual Property Code“, unless UNIVERSIGN has previously given its written agreement.

3.7.4 Personal data

UNIVERSIGN platform has been registered with the French board which enforces law on data protection (CNIL), in compliance with the enactments of law #78-17 of January, 6th, 1978 [CNIL].

Subscribers are informed that personal data they provide may be transferred and processed by UNIVERSIGN and its partners involved in the given exchanges, in compliance with article 32 of this law.

Subscribers are informed that they have the right to access, correct and delete the data regarding themselves by contacting UNIVERSIGN.

UNIVERSIGN takes all necessary measures to ensure that personal data are kept secure and confidential in accordance to French law #78-17 of January, 6th, 1978.

The UNIVERSIGN personnel are required to respect the enactments of French Law #78-17 of January, 6th, 1978.

They notably have no right to collect or to use in a misappropriate way the personal data they access, and generally speaking, to act in a way likely to be damaging to private life or to personal reputation.

UNIVERSIGN is bound to keep the informations provided by the Subscribers confidential, unless its disclosure is allowed by the Subscriber or demanded by regulation or adjudication.

3.8 Amendments

3.8.1 Procedure for amendment

UNIVERSIGN is responsible, through its Approval Board, for the creation, the approval, the maintenance and the modifications of the current TSP.

When a new version of the TSP is approved by the UNIVERSIGN Approval Board, it will be published on UNIVERSIGN web site and will replace the terms of the previous version.

3.8.2 Notification mechanisms and period

The only modifications that the Approval Board can perform on the current TSP without notification are minor changes. This includes, for instance, editorial or typographic changes, clarifications or corrections of obvious mistakes. The Approval Board can decide whether a modification is minor or not at its sole discretion.

For a non minor modification, the new TSP will be published for comments, with an indication of the proposed effective date.

When a new version of the TSP is published, all the Subscribers and Relying Parties of the UNIVERSIGN TSS are informed of the nature, the time and the date of change, through a publication on the UNIVERSIGN blog.

At the end of the comment period, the Approval Board can decide to publish the new TSP, the restart the amendment process with a new version or to withdraw the proposed version.

Unless otherwise stated, the new version of the TSP will take effect 14 working days after its publication and will remain in effect until a new version takes effect.

3.8.3 Circumstances under which OID must be changed

If the Approval Board determines that an OID change is necessary, the new version will indicate the new OID.

The Approval Board remains the only judge to determine if an OID change is necessary. An OID change is primarily used in case of a major change which can impact the insurance level of the TSTs already issued.

4 Operational requirements

4.1 Management of the TST requests

UNIVERSIGN provides a service for the management of the TST requests. The specific conditions of this service are described in the ToU accepted by the suscribers.

4.2 Audit log

Unless otherwise mentioned, UNIVERSIGN ensures that any appropriate information regarding the TSS operation is kept five (5) years after the corresponding TSU has been decommissioned, mainly in order to provide evidence in case of legal investigation.

Audit logs cover events relating to:

- generation of TST;

- administration of the TSS: context management, certificate import, service status;
- operation and synchronization of internal clock;
- TSU keys life cycle;
- TSU certificates life cycle;
- any kind of events which might impact the TSU operation.

Each audit record contains precise date and time of the event.

The audit log confidentiality is ensured by an appropriate management of physical, system and network access. The integrity is crytographically ensured.

The management of these records complies with the management of UNIVERSIGN classified information.

4.3 Private key life cycle management

UNIVERSIGN ensures that the private signing keys of the TSU are not used after the end of their life cycle.

The TSU automatically destroys the private key when the usage period of the key is reached. TSU keys are not renewed.

UNIVERSIGN ensures the the number of TSUs in operation at any given time is sufficient to provide a reliable service.

4.4 Clock synchronization

UNIVERSIGN ensures that its clocks are synchronized with the universal time (UTC) with the declared accuracy of one second.

More specifically:

1. the calibration of the TSU is maintained so that the clocks shall not be expected to drift outside the declared accuracy;
2. the TSU clocks are protected against threats related to their environment that could lead to a desynchronisation with respect to UTC time outside the declared accuracy;

3. UNIVERSIGN ensures that a TSU internal clock drift outside the bounds of the declared accuracy is detected. The detection of such a clock drift shall be published on UNIVERSIGN blog in order to inform Subscribers and Relying Parties;

4. if the clock of one of the TSU is detected as outside the declared accuracy, then TSTs will not be generated any more;

5. UNIVERSIGN ensures that clock synchronization is maintained when a leap second occurs as notified by the appropriate body. The change to take into account the leap second shall occur during the last minute of the day when the leap second is scheduled to occur. A record of the exact time (within the declared accuracy) is performed when this change occurs.

4.5 TST

UNIVERSIGN ensures that the TSTs are generated securely and include the correct time.

4.5.1 Content of a TST

In the answer to a Subscriber request, UNIVERSIGN provides a TST complying with the [RFC 3161] and containing the following fields:

version	Version 1
policy	OID : 1.3.6.1.4.1.15819.5.2.2
messageImprint	OID of the hash algorithm and the hash value of the data to time-stamp. Note : this information is provided by the Subscriber in the request.
serialNumber	160 bit random number uniquely identifying the request.
genTime	Time-stamp date in ASN.1 GeneralizedTime format
accuracy	Accuracy of 1 second
ordering	Flag set to FALSE
nonce	Value sent back identically if contained in the request
tsa	DN=[C=FR, O=Cryptolog International, OU=0002 43912916400026, CN=Universign Timestamping Unit xxx] where “xxx” is the serial number of this TSU. NB: This field is the same as the “subject” of the certificate used to sign the TST.
extensions	Not used.

4.5.2 TST signature

In accordance with section 6.7 of this document, the content of a TST is signed using a 2048 bit RSA private key.

4.6 TSA compromise

In the case of events impacting the security of the TSS and which could impact the generated TSTs, UNIVERSIGN ensures that appropriate information is provided to Subscribers and Relying Parties.

The TSA compromise could be caused by:

- the compromise of the TSU private keys;
- the compromise of the AC UNIVERSIGN private key used to generated the TSU certificates;
- an operational problem.

UNIVERSIGN has taken into account in its Disaster Recovery Plan the potentiel compromise of its TSS.

4.6.1 Disaster Recovery Plan

The Disaster Recovery Plan addresses the compromise of TSU private signing key, either actual or suspected, or the loss of calibration of a TSU clock, which might impact the issued TSTs.

UNIVERSIGN has signed a contract with the hosting provider of its TSS, which ensures that all necessary measures have been taken in order to avoid operational incidents.

UNIVERSIGN constantly updates its Disaster Recovery Plan in order to cover and to ensure the best possible service against the following threats:

- private key compromise;
- network failures;
- unavailability of qualified personnel;

- problems with clock calibration;
- failure of hardware components.

More generally, incidents on the TSS will be handled according the the incident management procedure in effect at UNIVERSIGN.

4.6.2 Communication

In case of a compromise, real or suspected, or the loss of calibration of a TSU, that could impact generated TSTs, UNIVERSIGN will provide Subscribers and Relying Parties with a description of the incident, in accordance with its Communication Plan. These informations are published on the web site: http://blogs.universign.eu

4.6.3 Interruption of TST generation

In case of a compromise, real or suspected, or the loss of calibration of a TSU, that could impact generated TSTs, UNIVERSIGN takes all necessary measures to ensure that this TSU does not generate any further TSTs until steps are taken to restore the situation.

4.6.4 Information on TST validity

In case of major compromise of UNIVERSIGN operation or loss of calibration which might impact the issued TSTs, whenever possible, UNIVERSIGN shall make available to all Subscribers and Relying Parties information which may be used to identify the TST which may have been impacted, unless this breaches the security of the TSS.

4.6.5 DGME alert

In case of a compromise, real or suspected, of its TSS, UNIVERSIGN will notify directly and without delay, the DGME contact point identified on the web site: http://www.references.modernisation.gouv.fr.

4.7 End of activity

Procedures to handle the end of activity are defined by UNIVERSIGN. Through these procedures, UNIVERSIGN ensures that potential disruptions to Subscribers and Relying Parties are minimized should the TSS cease activity. In particular,

UNIVERSIGN ensures that all the information necessary to verify the correctness of TSTs will be provided, even after the termination of its TSS.

Prior to the termination of its TSS, the following procedures will be performed:

- UNIVERSIGN will notify all its Subscribers and Relying Parties of the upcoming termination by publishing this information on its web site;
- UNIVERSIGN will terminate authorization of all subcontractors to act on its behalf in carrying out any functions relating to the process of issuing TST;
- UNIVERSIGN will transfer obligations to a reliable body for maintaining event logs and audit archives necessary to demonstrate its correct operation for a reasonable period;
- UNIVERSIGN will maintain its obligations to make available its public keys or certicates to relying parties for a reasonable period;
- the TSU private keys will be destroyed so that they cannot be retrieved, according to the procedure described in section 4.3.

UNIVERSIGN takes all necessary measures to cover the costs to fulfill these minimum requirements in case it becomes bankrupt or for other reasons is unable to cover the costs by itself.

The provisions made for termination of service include:

- notification to Subscribers and Relying Parties;
- transfer of UNIVERSIGN obligations to other bodies.

UNIVERSIGN will directly and immediately notify the DGME contact point identified on web site:
http:/www.references.modernisation.gouv.fr.

5 Facility, management, and operational controls

5.1 Physical controls

5.1.1 Site location and construction

UNIVERSIGN relies on secured premises to host its TSS. These premises feature locked rooms, cages and lockers.

5.1.2 Physical access

Access to TSS facilities is strictly restricted to authorized personnel listed on an access list. These authorizations are stated to the UNIVERSIGN hosting provider and a logbook is updated each time maintenance is performed on the TSS equipements. This logbook records the following information:

- the date and time of the operation;
- the last name and first name of the persons present;
- the description of the maintenance operation;
- the date and time of the end of the operation;
- the signature of the persons present.

Physical access is furthermore restricted by implementing mechanisms to control access into the high-security zones of the hosting provider. These mechanisms imply that authorized administrators own access cards.

The access security is strengthened by a biometric reader.

Access profiles to a zone are defined and maintained by the TSA and transfered to the hosting provider.

UNIVERSIGN secured areas are audited on a regular basis to verify that the access control systems are always operational and running. Monitoring and logging systems are implemented in all sites for all secured areas.

Access controls apply to all secured zones.

5.1.3 Power and air conditioning

Emergency controls are operated by the hosting provider so that a disruption of power supply, or an air conditionning failure do not jeopardize UNIVERSIGN commitments in terms of availability.

5.1.4 Water exposures

The specification of the security perimeter takes into account the risks related to water exposures. Protection controls are operated by the hosting provider in order to prevent from residual risks (pipe break for instance).

5.1.5 Fire prevention and protection

Secured areas benefit from appropriate prevention and protection against fire exposures.

5.1.6 Media storage

Media are stored securely. Backup media are securely stored in a separate location from the original media location.

All media storage areas are protected from fire, water exposure and damages.

Paper documents are kept by the TSS in secured locked premises and stored in a safe which opening means are known only by the TSA Chief Officer and authorized personnel.

5.1.7 Waste disposal

Materials listed as confidentially sensitive are subject to destruction, or can be used again in an similar operational context at the same level of sensitivity.

5.1.8 Off-site backup

In order to ensure a recovery complying with its commitments after an incident, UNIVERSIGN implements off-site backups of information and critical functions.

UNIVERSIGN ensures that backups are exported out of the production site and are protected as regards confidentiality and integrity.

5.2 Procedural controls

5.2.1 Trusted roles

The following Trusted Roles are defined:

- TSA Security Officer: has responsibility for all security issues of the TSS.
- TSA System Administrator: installs, configures and maintains the trustworthy systems of the TSS.
- TSA System Operator: responsible for operating the TSU on a day-to-day basis.

- TSA System Auditor: responsible for the day-to-day analysis of the audit logs.

Operations and supervisions are all performed by UNIVERSIGN personnel.

5.2.2 Number of persons required per task

The TSA enforces procedures to ensure that multiple person in a Trusted Role are required to perform sensitive tasks.

5.2.3 Identification and authentication for each role

Identification and authentication controls are defined in order to support the implementation of the access control policy and the acountability of operations. The access control policy limits access to authorized personnel on a need to know basis.

Personnel in trusted roles are appointed with written notifications.

5.2.4 Roles requiring separation of duties

UNIVERSIGN ensures that security procedures are separated from standard exploitation procedures and that they are always performed under the supervision of a personal in a trusted role.

5.2.5 Risks analysis

A risk analysis is carried out on the TSS in order to identify the threats on the TSU.

5.2.6 System access management

Identification and authentication:
Systems, applications and databases uniquely identify and authenticate operators and administrators. Any interaction between the system and an operator is possible only after successful identification and authentication. For any interaction, the system checks the identity of the operating personnel.

Authentication informations are stored in a way they can only be access by authorized users.

Access control:
Profiles and access rights to the TSA equipements are specified and documented, as well as the registration/deregistration procedures of operating personnel.

Systems, applications and databases can distinguish and manage the access rights for each user on objects subject to rights management, at user level, at group level, or both. It is possible to:

- deny users or groups of users the access to an object;
- limit user access to an object to operations which do not modify this object;
- grant access rights to an object with the granularity level of the individual user.

Someone who is not an authorized user cannot grant nor deny access rights to an object. Likewise, only authorized users are allowed to create new users, and to suppress or suspend existing users.

Administration and operation:
Usage of utility tools is restricted and controlled.

5.2.7 Operation management

System planning:
Systems load are monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.

Protection against malicious codes:
Monitoring, detection and prevention are implemented on every component of the TSS so as to provide protection against malicious softwares.

Network security controls:
Implemented controls comply with the strategy of UNIVERSIGN risks management for information systems.

The TSS is implemented on a network protected firewalls. These firewalls are configured to accept only connections which are strictly necessary.

The network communications transfering confidential information are protected against eavesdropping.

Security controls are implemented in order to protect the local components of the information system from non-authorized access.

Media handling and security:
All sensitive media of the TSS are subject to maintenance procedures in order to ensure the availability of functions and information.

End of life conditions (destruction and waste disposal) of equipements are documented in order to ensure the non-disclosure of sensitive information they may enclose.

Exchange of information:
Security controls are implemented in order to ensure the authentication of origin, the integrity and the confidentiality, when necessary, of exchanged data between parties involved in the process.

5.2.8 Trustworthy systems deployment and maintenance

The TSS use trustworthy components. In particular, the TSUs meet the regulatory requirements. The TSA Approval Board is notified of any substancial change of the system.

Releases are subject to an update of the operational procedures. Controls of maintenance operations are implemented.

Proper performance of applications:
The development and test infrastructures are separated from the operational infrastructures of the TSS.

Criteria of acceptance and validation of new systems, upgrades and new versions are documented and appropriate tests are performed before acceptance and production step.

5.2.9 Incident reporting and response

Operation monitoring is possible through the audit logs.

Any TSU malfunction is immediatly notified to the supervisor and operator of the UNIVERSIGN platform. These notifications notably regard:

- Start / stop of services;
- Desynchronisation of the TSS clocks;
- TSS network problems.

Each event is stored in a database from which all service events, including incidents, can be traced.

If an incident occurs, UNIVERSIGN will act in an appropriate way in order to react rapidly, to limit the impact of security exposure and to restore the service in the best possible time.

5.3 Personnel controls

UNIVERSIGN has documented information security for human resources. UNIVERSIGN notably states that personnel in a Trusted Role of the TSS are carefully selected and clearly informed of operations and rules to be followed.

5.3.1 Qualifications, experience, and clearance requirements

Any person in a Trusted Role is subject to a clause of confidentiality, managed by UNIVERSIGN. UNIVERSIGN ensures that the professional skills of personnel in Trusted Roles comply with the requirements of their functions. UNIVERSIGN management has appropriate expertise, and is familiar with security procedures. Any person in a Trusted Role is informed of his responsibility through its job description and/or procedures related to system security and personnel control.

Personnel working on the UNIVERSIGN TSS possess appropriate knowledge of:

- time-stamping technology;
- digital signature technology;
- mechanisms for calibration or synchronization of the TSU clocks with UTC;
- security procedures, for personnel with security responsibilities;
- information security and risk assessment.

5.3.2 Background check procedures

UNIVERSIGN performs a background check prior to recruiting new personnel, in order to ensure the suitability with the open position.

5.3.3 Training requirements

Personnel is trained regarding softwares and hardwares in use and regarding the application of internal procedures.

5.3.4 Retraining frequency and requirements

Each change of systems, procedures or organization results in information or training of the operating personnel when this change impacts the work of this category of personnel.

Operating personnel are trained regarding incident management and escalation.

5.3.5 Job rotation frequency and sequence

Not applicable.

5.3.6 Sanctions for unauthorized actions

Sanctions in case of unauthorized actions are listed in an IT charter and through the document regarding information security for human resources. All UNIVERSIGN personnel are informed of these sanctions.

5.3.7 Independent contractor requirements

Requirements towards subcontractors are subject to contracts.

The commitments include contracts relating to service supply, non-disclosure agreements and IT charter.

5.3.8 Documentation supplied to personnel

Personnel are informed of the security rules related to their role as soon as they are appointed. Person in charge of an operational role in the TSS are provided with related procedures.

6 Technical security controls

6.1 Time accuracy

TSU clocks are locally monitored by reference time servers. These servers are autonomous and are synchronized with UTC(k) reference servers. The mechanisms used allow the system to withstand attacks aiming at desynchronizing time sources, even major attacks against radio or satellite signals.

UNIVERSIGN ensures that the TSTs generated by its TSS have an accuracy with respect to UTC time of less than one second.

6.2 Key generation

UNIVERSIGN ensures that all cryptographic keys are generated in a controlled environment. Specifically, TSU signing keys are generated within a time-stamping module conforming to the state of the art.

The generation of TSU cryptographic keys is performed within hardware security modules. TSU private keys are never exported outside of these modules.

The TSUs use 2048 bit RSA private keys.

6.3 Certification of TSU keys

A TSU certificate request is transmitted to the UNIVERSIGN CA, in accordance with the rules defined in the corresponding Certificate Policy [**UCP**].

The certificates delivered by the CA conform to the profile defined in the Certicate Policy.

The TSA abides by its obligations defined in the Certificate Policy of the CA.

The TSA verifies, when importing a certificate in a TSU, that it comes from the UNIVERSIGN CA.

6.4 Protection of TSU private keys

UNIVERSIGN ensures that the TSU private keys are kept confidential and garantees their integrity. Specifically, the TSU signing keys are kept and used within time-stamping module following the state of the art.

6.5 Backup of TSU private keys

UNIVERSIGN forbids the archival and backup of TSU private keys.

6.6 Destruction of TSU private keys

UNIVERSIGN ensures that TSU private keys are destroyed at the end of their life cycle.

6.7 Mandatory algorithms

The UNIVERSIGN TSA:

1. accepts hash values generated by Subscribers and using hash algorithms in compliance with regulatory requirements. The accepted hash algorithms are the following:
   - SHA-1[1]
   - SHA-256
   - SHA-384
   - SHA-512
2. issues TSTs signed with algorithms and key lengths in compliance with regulatory requirements. The TSU key pair is an 2048 bit RSA key. The signature algorithm uses an hash fonction belonging to the SHA-2 family.

6.8 TST verification

UNIVERSIGN ensures that Relying Parties can obtain information needed to verify the digital signature of TSTs. UNIVERSIGN notably ensures that the TSU certificates are available, either attached to the TSTs or from the UNIVERSIGN web site: http://docs.universign.eu.

6.9 Validity period of TSU certificates

A TSU certificate is valid for six (6) years. UNIVERSIGN ensures that the algorithm and the key size are known to be adequate for this validity period.

[1] Usage of this algoritm is still accepted for compatibility reasons. While no practical attack has been publicy disclosed, this algorithm is currently considered weak. It is recommended to use one of the other algorithms in the list.

6.10 Usage period of TSU private keys

The private key linked to the TSU certificate and which signs TSTs has a usage period of one year.

Considering that the validity period of a TSU certificate is 6 years, Subscribers and Relying Parties can verify the validity of TSTs for at least five (5) years after their generation.

7 Certificate and TST profiles

7.1 Certificate profile

Base fields

Field	Value
Version	2
Serial Number	defined by the CA
Signature	RSA/SHA-256
Issuer DN	C=FR, O=Cryptolog International, OU=0002 43912916400026, CN=Universign Timestamping CA (or Universign Timestamping CA 2015)
Validity	6 years
Subject DN	C=FR, O=Cryptolog International, OU=0002 43912916400026, CN=Universign Timestamping Unit xxx
Public Key	RSA 2048 bits

Certificate extension

Field	OID	Critical	Value
Authority Key Identifier	2.5.29.35	No	
KeyIdentifier			RFC 5280 - Method 0
Key Usage	2.5.29.15	Yes	
digitalSignature			True
nonRepudiation			False
keyEncipherment			False
dataEncipherment			False
keyAgreement			False
keyCertSign			False
cRLSign			False
encipherOnly			False
decipherOnly			False
Certificate Policies	2.5.29.32	No	
policyIdentifier			1.3.6.1.4.1.15819.5.1.1
policyQualifierId			1.3.6.1.5.5.7.2.1
qualifier			http://docs.universign.eu/
Basic Constraint	2.5.29.19	Yes[2]	
CA			False
Maximum Path Length			Absent
Extended Key Usage	2.5.29.37	Yes	
KeyPurposeId			id-kp-timeStamping
CRL Distribution Points	2.5.29.31	No	
fullName			http://crl.universign.eu/tsa_root.crl
reasons			Absent
cRLIssuer			Absent

7.2 TST profile

version	Version 1
policy	OID : 1.3.6.1.4.1.15819.5.2.2
messageImprint	OID of the hash algorithm and the hash value of the data to time-stamp. Note : this information is provided by the Subscriber in the request.
serialNumber	160 bit number uniquely identifying the TST
genTime	Time-stamp date in ASN.1 GeneralizedTime format

[2]This CP authorise to set the criticity parameter to `No` to be in conformity with RGS requirement.

accuracy	Accuracy of 1 second
ordering	Flag set to FALSE
nonce	Value sent back identically if contained in the request
tsa	DN=[C=FR, O=Cryptolog International, OU=0002 43912916400026, CN=Universign Timestamping Unit xxx] where "xxx" is the serial number of this TSU. NB: This field is the same as the "subject" of the certificate used to sign the TST.
extensions	Not used

8 Compliance audit and other assessments

8.1 Frequency or circumstances of assessment

Two kinds of compliance audit are made:

- an internal audit performed at least once a year
  - by an external provider specialized in TSS; or
  - by an internal auditor.
- a qualification audit performed by an accredited organization at least once a year.

During the RGS qualification process, a first compliance audit has been performed by the society LSTI as requested by the regulatory proceeding.

An audit ensuring compliance to this TSP shall be performed

- at the start of the SH
- at least once a year for internal audit
- during annual renewal of qualification, as requested by the regulatory proceeding.
- after each major modification.

During the RGS qualification process, a first compliance audit has been performed by the society LSTI as requested by the regulatory proceeding.

8.2 Identity/qualifications of assessor

The assessor must act with rigor in order to ensure that policies, statements and services are properly implemented and to detect the non-compliance items which might jeopardize the security of the service.

The TSA commits to hire assessors with a high level of expertise in system security, particularly in the field of the audited component.

8.3 Assessor's relationship to assessed entity

The assessor is appointed by UNIVERSIGN, and is allowed to audit the practices ruling the target component of the audit. He may be part of UNIVERSIGN but is independant from the TSA.

8.4 Topics covered by assessment

The assessor operates compliance audits of the specified component, covering totally or partly the implementation of:

- the TSP;
- the TSPS;
- the TSS.

Prior to every audit, the assessor will provide the TSA Approval Board with a list of components and procedures they wish to audit, and will subsequently prepare the detailed audit program.

8.5 Actions taken as a result of deficiency

Following the compliance audit, the assessment team gives the TSA the result which can be "success", "failure" or "to be confirmed".

In case of failure, the assessment team delivers recommendations to the TSA. The TSA then decides which actions to perform.

In case of result "to be confirmed", the assessment team identifies the non-compliances and prioritizes them. The TSA then schedules the correction of these non-compliances. A validation audit then checks for their effective corrections.

In case of success, the TSA confirms that the audited component complies with the requirements of the TSP.

8.6 Communication of results

The audit results are made available to the Approval Board of the TSA and to the qualification organism in charge of the qualification of the TSA.

References

[**ORD**]
Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

[**RFC 3161**]
IETF RFC 3161 - Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)

[**UCP**]
UNIVERSIGN CA Certificate Policy. OID:1.3.6.1.4.1.15819.5.1.2

[**ETSI TSP**]
ETSI TS 102 023 V1.2.1 (2003-01) - Policy requirements for Time-Stamping Authority

[**RGS_A_12**]
Référentiel Général de Sécurité - Politique d'Horodatage Type - Version 2.3 - 18/02/2010. OID:1.2.250.1.137.2.2.1.2.2.4

[**CNIL**]
Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004.