Universign Timestamping CA

Certification Policy

OID: 1.3.6.1.4.1.15819.5.1.1

VERSION : 2.1	DISTRIBUTION : *PUBLIC*	Effective date : 01/07/2016

Contents

1 Introduction

1.1 Overview

UNIVERSIGN is a Trusted Service Provider (TSP) for its own needs, notably for the needs of its qualified Time-Stamping Service (TSS).

The organization chosen for that purpose is presented in chapter 1.3.

Scope of this CP/CPS The Universign Trusted Network is presented [1] in Figure 1. The scope of this CP focuses on Primary AC and delivering certificates to Time-Stamping Units.

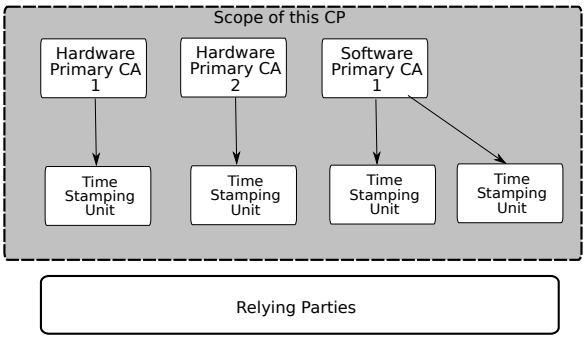

Figure 1: Universign Trusted Network and scope of this CP/CPS

This Certificate Policy (CP) defines UNIVERSIGN commitments regarding the issuance of certificates for its own TSS, in accordance with

- the standard CP of the French RGS "Cachet". UNIVERSIGN aims to be accredited at the level * of this document;
- ETSI EN 319 411-1 level NCP+.

Universign defined certification practices statements and processes according to the current CP.

[1] This figure is provided for descriptive purposes. The CAs used are not the one shown by the figure.

1.2 Document name and identification

This document is UNIVERSIGN Certification Policy. This CP is identified, within the documentation framework of UNIVERSIGN trust architecture, by a unique identification number: **1.3.6.1.4.1.15819.5.1.1**

1.3 PKI participants

1.3.1 Certification Authorities

In the French regulatory context, a Certification Authority (CA) and a Certification Service Provider (CSP) 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 CSP is a specific kind of PSCO. A CSP is defined as a person or an entity responsible for the generation of the management of certificates, with respect to its Subscribers and Relying Parties. A CSP includes at least one CA, but could have several depending on its organization. A CSP is identified in the certificates under its responsibility through the CA which has issued this certificate and whose name is included in the "issuer" field of the certificate.

Within a CSP, a CA is in charge, in name of and under the responsibility of the CSP, of the application of at least one CP. In the scope of this CP, the term CSP is not used outside this section and section 1.1 and only the term CA is used. It designates the UNIVERSIGN CA in charge of applying this CP, within the UNIVERSIGN CSP.

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

The board has the final authority and responsibility for:

- specifying and approving the PKI and the practices;
- approving the CP and the CPS;
- defining the update process of the CPS and the CP, with the responsibility of the maintenance of the CPS and the CP;
- defining the review process ensuring that UNIVERSIGN correctly abides by the practices defined in the CPS;

- defining the review process ensuring that the CP is enforced by the CPS;
- publishing the CP and the public part of the CPS (included in this CP), as well as their revisions, to Subscribers and Relying Parties.

1.3.2 Registration Authorities

For the purpose of issuing certificates for its own servers, UNIVERSIGN is its own Registration Authority (RA).

1.3.3 Subscribers (Sealing Certificate Officers)

In the scope of this CP, a Subscriber, also called Sealing Certificate Officer (SCO), is an individual responsible for the usage of the server certificate issued, on behalf of the entity identified in this certificate. The SCO belongs to this entity.

If the SCO leaves the entity or changes position, a new SCO must be appointed immediately.

1.3.4 Relying parties

A Relying Party is anyone, either an entity or a physical person, whose activities will depend on the validity of a certificate issued by a primary CA, particularly the association between the TSU and the public key. A Relying Party is responsible for deciding how to check the validity of a TSU Certificate, at least by checking the appropriate certificate status information. A Relying Party may use information in the Certificate (such as Certificate Policy identifiers) to determine the suitability of the Certificate for a particular use.

1.3.5 Other Participants

The Primary Trusted Parties are individuals or entities with strong implication in the UTN or which, due to their status, have a specific relationship with Universign. A Primary Trusted Party may be (but is not limited to):

- Software publishers with trusted certificate stores;
- Owners of Trust-Service Status List (TSL);
- Government bodies.

Universign maintains a list of the Primary Trusted Parties and notifies them when major events occur during the CA life cycle.

PKI components All components of the PKI (CA, RA, Subscribers) are managed and operated by UNIVERSIGN.

Certification Representatives This CP does not define Certification Representatives.

1.4 Certificate Usage

1.4.1 Appropriate certificate uses

Key pairs and certificates of servers This CP deals with keys and certificates used by UNIVERSIGN Time-Stamping Units (TSUs). The TSUs use the key pairs to sign the TSTs they issue, so that the Relying Parties can verify the signature.

Key pairs and certificates of the CA and its components The certificates of the CA defined by this CP are used to sign:

- the TSU certificates of UNIVERSIGN TSS;
- the CRLs of the CA.

The CA has a single certificate signing key pair active at a time and the corresponding certificate is a root certificate. This certificate is self-signed and is not related to an higher level CA.

1.4.2 Prohibited certificate uses

Any usage other than those defined in the previous paragraph is prohibited by this CP.

1.5 Policy administration

1.5.1 Organization administering the document

UNIVERSIGN
Cryptolog International
7 rue du Faubourg Poissonnière, 75009 Paris, France
contact@universign.eu

1.5.2 Contact person

Questions concerning this CP should be sent to:

The Certificate Policy Manager
UNIVERSIGN
Cryptolog International
7 rue du Faubourg Poissonnière, 75009 Paris, France
contact@universign.eu

1.5.3 Person determining CP suitability for the policy

UNIVERSIGN is responsible for controlling the conformance of the CP and the documented practices.

1.5.4 CP approval procedures

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

1.6 Definitions and acronyms

Definitions

The terms used in this CP are the following:

Certificate
: Electronic document issued by Universign including the identity of the Certificate holder and a mathematical key known as public key used to control the identity of the Certificate holder.

Certification Authority
: Authority in charge of the application of the Certification Policy, the issuing and management of the Certificates. As part of this CP, the Certification Authority is Universign.

Certification Policy
: The current document, involving all the commitments of Universign in terms of security and organisation regarding its Certificates issuing service.

Certificate Revocation List
: List of Certificates that have been revoked, and therefore should no longer be trusted.

Object Identifier
: Unique identifier assigned by a known standardisation authority (AFNOR in France). It is then developed by Universign to identify his documents in a unique way.

Public Key Infrastructure
: Set of components providing certificates and keys management services for a user community.

Time-Stamping Authority
: Entity responsible for applying a Time-Stamping Policy, by using one or more TSUs. The Time-Stamping Authority delivers Time-Stamp Tokens with a specified accuracy from chosen time sources.

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

Universign
: Trade name of the company Cryptolog International, SAS with a capital of 504 932 euros, 7, Rue du Faubourg Poissonnière, 75009 Paris, France, registered with the Paris Registry of Companies under the number 439 129 164.

Acronyms

The acronyms used in this CP are the following:

CA: Certification Authority

CP: Certification Policy

CRL: Certificate Revocation List

CSP: Certification Service Provider

DN: Distinguished Name

HSM: Hardware Security Module

OID: Object Identifier

PKI: Public-Key Infrastructure

RA: Registration Authority

RGS: Référentiel Général de Sécurité

SCO: Sealing Certificate Officer

TSA: Time-Stamping Authority

TSU: Time-Stamping Unit

TST: Time-Stamp Token

2 Publication and repository responsibilities

2.1 Repositories

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

Informations related to certification practices meant to be publicly distributed are included in this CP.

2.2 Publication of certification information

The Primary CAs must publish at least the following information:

- this CP [2];
- the applicable CRLs, as published in accordance with the Requirements of this CP;
- the active certificate of the Universign Primary CAs containing the public key corresponding to their private signing key, and their hash;
- the Relying Parties Agreement;

The CA provides to the SCOs, who are internal staff members of UNIVERSIGN, the requirements and responsibilities of each participants through this CP.

The availability of publication site is 24/7 under normal conditions.

[2] Copies of past versions of this CP and their effective period are available on demand.

2.3 Time or frequency of publication

A new CP will be published when:

- substantial modifications of the CPS have an impact on this CP;
- regulatory evolutions have an impact on this CP;

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

The CRLs are published at most 24 hours after a revocation request.

2.4 Access Controls on repositories

The published informations are published on the UNIVERSIGN web site and can be freely read by anyone. The CP and the CRLs 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 by authorized UNIVERSIGN personnel, through access control.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of names

Names used conform to the specifications of the X.500 norm.

The CA and the TSU are identified by an explicit name (called "DN" hereafter) of type X.501. This type of DN is defined in chapter 7.

3.1.2 Need for names to be meaningful

The DN of the UNIVERSIGN CA is specified in chapter 7.
The DN of a UNIVERSIGN TSU is specified in chapter 7.

3.1.3 Anonymity or pseudonymity of subscribers

Not applicable.

3.1.4 Rules for interpreting various name forms

The interpretation rule of DN field of the issued certificates is in conformity with [RGS_A_14].

The interpretation is performed as follows:

Field	Interpretation
C	Company country identifier of the company operating the time-stamping service
O	Name of the company operating the time stamping service
OU	Country code of the company registration followed by the company registration unique ide
CN	Unique identifier of the Time-stamping Unit

UNIVERSIGN, as a CA, issues certificates only for its own timestamping units[3], therefore, in practice, the above fields of the DN are fixed. Thus, the field shall be interpreted as follow:

Field C Field C contains value FR, i.e. the country code of UNIVERSIGN registration.

Field O Field O contains Cryptolog International, official name of the company operating UNIVERSIGN time stamping service.

Field OU Field OU contains the following elements:

- 0002, ICD of France, followed by a space, and followed by
- 43912916400026, i.e. SIRET number (French company unique identifier) of CRYPTOLOG INTERNATIONAL company

champ CN Time stamping units are identified by a number, then the CN field:

Universign Timestamping Unit xxx

shall be interpreted as xxxth *Universign Time Stamping Unit* where xxx is a 3 digits number [4]. Each time a new certificate is issued, the number is incremented.

3.1.5 Uniqueness of names

UNIVERSIGN, as a CA, ensures that the identifier of the TSU, embedded in the CN field of the certificate, is incremented for each new installation of a TSU certificate. UNIVERSIGN bears the responsibility to verify and establish unique names for its TSU certificates.

[3] For future versions of this CP, UNIVERSIGN *may* be allowed to issue certificates for third parties time stamping services, as long as they are compliant with requirements of this CP.

[4] from 001 to 999

3.1.6 Recognition, authentication, and role of trademarks

Not applicable.

3.2 Initial identity validation

The registration of a TSU to which a certificate must be issued is performed through the registration of the SCO. This person is necessarily part of UNIVERSIGN personnel.

The identity of the SCO is clearly established in the CPS. The SCO must be identified by and registered with the CA before his request can be handled.

After being registered with the CA, the SCO can request the issuance of certificates for TSUs belonging to UNIVERSIGN.

The SCO is present during the generation of a TSU key.

3.2.1 Method to prove possession of private key

Not applicable.

3.2.2 Authentication of organization identity

See below.

3.2.3 Authentication of individual identity

In the scope of this CP, it is the registration of a SCO without Certification Representative. He is necessarily part of UNIVERSIGN personnel. Universign only requires the elements needed to issue the certificate.

In order to request the issuance of a certificate for a TSU, the SCO must be registered with the CA by:

- Filling and submitting to the CA Chief Officer the signed SCO registration form;
- Providing a authorization signed by his legal representative;
- Providing a copy of an official ID document including a recent picture, the place and date of birth of the subject;

- Reading this CP and most notably the SCO obligations. He must also sign this CP.

All these items make up the registration file of a SCO and are kept by the CA in a safe.

The registration of a SCO is necessarily performed through a physical meeting between the CA Chief Officer and the SCO.

If the SCO changes, the CA requires the nomination of a new SCO who will become responsible for the certificates attached to the previous SCO. A SCO change requires a complete registration procedure as described above.

3.2.4 Non-verified subscriber information

Not applicable.

3.2.5 Validation of authority

The requester must be an SCO registered with the CA as defined above.

3.2.6 Criteria for interoperation

This CP is for an internal CA of UNIVERSIGN and does not define any specific interoperation criteria.

3.3 Identification and authentication for re-key requests

The UNIVERSIGN CA does not perform such renewals.

3.3.1 Identification and authentication for routine re-key

Not applicable.

3.3.2 Identification and authentication for re-key after revocation

Not applicable.

3.4 Identification and authentication for revocation request

The revocation request is performed by the SCO by filling the revocation request form. The form includes the personal data of the SCO and is transmitted signed to the CA Chief Officer.

In order to validate the request, the CA ensures that:

- the SCO is correctly registered with the CA;
- the request is signed by the SCO. The CA matches the signature with the one recorded in the registration documents of the SCO;
- the identification of the TSU included in the revocation request is valid.

If the conditions above are met, the CA signs the revocation request and transmits it to the UNIVERSIGN exploitation teams who perform the technical steps for revocation.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate application

4.1.1 Who can submit a certificate application

The SCO responsible for a TSU within UNIVERSIGN performs the certificate request for this TSU by filling the TSU registration request form.

4.1.2 Enrolment process and responsibilities

The registration request of a TSU to a CA requires the following steps:

- the SCO completes a Certificate Application Form filled with correct information. The SCO shall provide all elements of the registration record, in particular :
  - The geographical location where the TSU will be integrated;
  - The DN identifying the TSU;
  - The technical information of the certificate: key size, algorithms.
- the TSU shall generate its own key pair;
- the SCO shall provide the public key of the TSU to the CA;

- the SCO shall provide evidence that he owns the private key associated with the public key.

To be valid, the request must be signed by the SCO and its legal representative.

Universign ensures that registration process is performed in accordance with applicable laws.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

The certificate requests for a TSU are validated by the CA which handles the RA function itself.

4.2.2 Approval or rejection of certificate applications

If the request is rejected, the SCO is immediately informed of the reason.

4.2.3 Time to process certificate applications

The CA begins processing certificate applications within a reasonable time of receipt. A certificate application remains active until rejected.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

The UNIVERSIGN CA is an off-line CA which is not connected to the network.

The UNIVERSIGN CA creates a certificate after the validation of the certificate request defined in section 4.2. The certificate is issued in accordance with the information provided in the certificate request and the profile defined in section 7.1. Certificate is generated within secure premises by two members of staff in a Trusted Role.

People in trusted roles with certificates issuing capabilities must use multi factors authentication.

The public key of the TSU shall by given to the Primary CA during a physical meeting and in a secured way.

4.3.2 Notification to subscriber by the CA of issuance of certificate

See above.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

Upon installation of the certificate on the TSU, the SCO verifies the data contained in the certificate and validates the correctness of the content. The verification concerning the installed certificate are also technically performed by the TSU.

In case of errors in the generated certificate, it would be immediately revoked and a new certificate generation procedure would take place.

4.4.2 Publication of the certificate by the CA

UNIVERSIGN publishes the TSU certificate at the following url: http://docs.universign.eu

4.4.3 Notification of certificate issuance by the AC to other entities

Not applicable.

4.5 Key pair and certificate usage

The certificate shall be used in compliance with:

- the requirements of the PC, in particular usages defined in section 1.4;
- the KeyUsage extension defined in certificate.

A TSU shall:

- protect its private keys.
- if its private keys are compromised, the use of the TSU private key is immediately and permanently discontinued and the fact of this compromised shall immediately be notified to the issuing primary CA.
- if the private key of the primary CA that issued the certificate has been compromised, the TSU shall no longer use its certificate.

4.6 Certificate renewal

Certificate renewal is not allowed by the UNIVERSIGN CA.

4.6.1 Circumstance for certificate renewal

Not applicable.

4.6.2 Who may request renewal

Not applicable.

4.6.3 Processing certificate renewal requests

Not applicable.

4.6.4 Notification of new certificate issuance to subscriber

Not applicable.

4.6.5 Conduct constituting acceptance of a renewal certificate

Not applicable.

4.6.6 Publication of the renewal certificate by the CA

Not applicable.

4.6.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.7 Certificate re-key

Certificate re-key is not allowed by the UNIVERSIGN CA.

4.7.1 Circumstance for certificate re-key

Not applicable.

4.7.2 Who may request certification of a new public key

Not applicable.

4.7.3 Processing certificate re-keying requests

Not applicable.

4.7.4 Notification of new certificate issuance to subscriber

Not applicable.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Not applicable.

4.7.6 Publication of the re-keyed certificate by the CA

Not applicable.

4.7.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.8 Certificate modification

The modification of a certificate is performed by revoking it and then performing a new initial certificate request.

4.8.1 Circumstance for certificate modification

Not applicable.

4.8.2 Who may request certificate modification

Not applicable.

4.8.3 Processing certificate modification requests

Not applicable.

4.8.4 Notification of new certificate issuance to subscriber

Not applicable.

4.8.5 Conduct constituting acceptance of modified certificate

Not applicable.

4.8.6 Publication of the modified certificate by the CA

Not applicable.

4.8.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

The causes for revocation of a TSU certificate are the following:

- the informations regarding the TSU included in the certificate are not accurate any more;
- the SCO has not abode by his requirements with respect to this CP and the certificate usage rules;
- suspected compromise, loss or theft of a private key;
- error in the registration procedure;
- end of activity of the CA.

4.9.2 Who can request revocation

The person who can request revocation of a TSU certificate are:

- the CA Chief Officer;
- the SCO.

4.9.3 Procedure for revocation request

The revocation request is validated by the CA Chief Officer.

The revocation request is submitted by the SCO and contains the following information:

- the DN of the TSU certificate to revoke;
- personal details of the SCO;

- possibly the reason for revocation. This reason is for information purposes and is not listed in the CRL.

The handling of the request is performed by an authorized person within the CA.

The CA informs the revoked certificate SCO of the change of status of its certificate. Revocations are definitive.

4.9.4 Revocation request grace period

The revocation request is submitted as soon possible.

4.9.5 Time within which CA must process the revocation request

The maximum handling period is 72 hours, although requests will usually be processed without delay.

4.9.6 Revocation checking requirements for relying parties

Relying Parties must verify the status of the certificate and the corresponding chain.

4.9.7 CRL issuance frequency

The frequency for publication of CRLs is 60 minutes.

4.9.8 Maximum latency for CRLs

CRLs are published at most 30 minutes after their generation.

4.9.9 On-line revocation/status checking availability

Not applicable.

4.9.10 On-line revocation checking requirements

Not applicable.

4.9.11 Other forms of revocation advertisements available

Not applicable.

4.9.12 Special requirements regarding key compromise

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

4.9.13 Circumstances for suspension

Certificate suspension is not authorized by this CP.

4.9.14 Who can request suspension

Not applicable.

4.9.15 Procedure for suspension request

Not applicable.

4.9.16 Limits on suspension period

Not applicable.

4.10 Certificate status services

4.10.1 Operational characteristics

The CRLs are in v2 format and posted on a publication site freely accessible within UNIVERSIGN.

Universign ensures the integrity and authenticity of published CRLs. CRLs include information on the status of certificates at least until the certificate expires.

4.10.2 Service availability

The Certificate Status Service is available on several publication servers ensuring an availability of 24x7 under normal operations.

In all cases, the CA ensures that a CRL will not be unavailable:

- more than 4 consecutive hours during working days;
- more than a total of 32 hours per month during working days.

4.10.3 Optional features

Not applicable.

4.11 End of subscription

If the relationship between the SCO and the CA ends, the responsibility of the corresponding certificates is transferred to a new SCO.

4.12 Key escrow and recovery

Keys are not escrowed.

4.12.1 Key escrow and recovery policy and practices

Not applicable.

4.12.2 Session key encapsulation and recovery policy and practices

Not applicable.

5 Facility, management, and operational controls

Universign defined his Information Security Policy. It describes the approach and the solutions to set up to manage the security.

The ISP is regularly updated and approved by Universign's management.

5.1 Physical controls

5.1.1 Site location and construction

UNIVERSIGN relies on secured premises to host its CA. The site location and construction, combined with other physical security protection mechanisms described hereafter, provides robust protection against unauthorized access to the CA equipment and records.

Secured facilities consist of several successive physical areas. Going from one secured area to the next one is only possible through a secured access, such as a door with an access badge or biometric control. This allows a strict access control to the secured area, limiting access to only authorized persons. Each secured zone is encapsulated in the preceding one, thus, each secured zone provides a more restricted access and a higher overall security level than the preceding one.

Especially, PKI root components are physically isolated from other components.

5.1.2 Physical access

Access to CA facilities is strictly restricted to authorized personnel listed on an access list. These authorizations are stated to UNIVERSIGN host and a logbook is updated each time maintenance is operated on the CA equipments. 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 person present.

Physical access is furthermore restricted by implementing mechanisms to control access into the high-security zones of the host. These mechanisms imply that authorized administrators own access cards. In order to access these secured areas, two administrators are required, along with their smart cards .

The access security is strengthened by a biometric reader.

Access profiles to a zone are defined and maintained by the CA and transferred to the host.

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 host so that a disruption of power supply, or an air conditioning 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 host 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 CA in secured locked premises and stored in a safe which opening means are known only by the CA 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 performed by Trusted Role.

Universign ensures that backups are exported out of the production site and are protected as regards confidentiality and integrity. Universign ensures that back-up are regularly tested to ensure that they meet the requirements of business continuity plans.

5.2 Procedural controls

5.2.1 Trusted roles

The Primary CA operates its own PKI. The Trusted Roles defined herein apply to all components of the PKI.

The following Trusted Roles are defined:

Security Officer: he or she has responsibility for all security issues of the system and operations of the PKI. As member of the Approval Board, he approves the generation and revocation of certificates;

System Administrators: he or she is in charge of the administration and configuration of all PKI technical components. He is also responsible for operating the CA trustworthy systems on a day-to-day basis. He is authorized to perform system backup and recovery;

System Auditors: authorized to day-to-day review archives and audit logs of the CA trustworthy systems.

Key custodian: ensures the confidentiality, the integrity and the availability of the secret shares that he was provided.

Primary CA personal in Trusted Role (and more generally, all Primary CA personal) shall be free of conflicting interests that might prejudice the impartiality of the operations.

Personnel in trusted roles are appointed with written notifications by Primary CA senior management. Universign regularly ensures that all the trusted roles are filled in order to guarantee the activity continuity.

5.2.2 Number of persons required per task

Each Primary CA enforces procedures to ensure that multiple persons in a Trusted Role are required to perform sensitive tasks such as PKI restart, key restore operations or certificates generation.

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 accountability 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

The CA ensures that the Security Officer and the System Administrator roles are not shared by the same person.

The CA ensures that security operations are separated from standard operation procedures and that they are always performed under the supervision of a person in a Trusted Role.

5.2.5 Risk analysis

A risk analysis is carried out by Universign in order to identify the threats on the primary CAs and TSUs. This risk analysis is periodically reviewed and each time a structural change occurs on a primary CA or TSU. Moreover, the risk analysis methodology allows Universign to ensure that its inventory is kept up to date.

5.3 Personnel controls

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.

5.3.2 Background check procedures

UNIVERSIGN performs a legal and professional background check prior to assign personnel to a Trusted Role, in order to ensure the suitability with the open position. This includes that:

- the personnel is free from conflict interests;
- the personnel does not have a conviction for a serious crime or other offence.

UNIVERSIGN selects the persons filling the Trusted Roles on the basis of loyalty, trustworthiness and integrity. Background checking are done in accordance with applicable laws.

5.3.3 Training requirements

Personnel is trained regarding software and hardware in use and regarding the application of internal procedures. Training material is maintained with respect to the practices.

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.

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. Persons in charge of an operational role in the PKI are provided with related procedures. Personnel shall exercise administrative and operational procedures in line with this documentation. Security rules and related procedures are validated by the Approbation Board.

5.4 Audit logging procedures

5.4.1 Types of events recorded

UNIVERSIGN ensures that the following events are recorded:

- system events from the different components of the PKI (server start, network access, ...);
- technical events from the PKI software;
- functional events from the PKI software (certificate request, validation, revocation ...);
- operations including authentication action from people with a trusted role.

The UNIVERSIGN CA is an off-line CA which events are stored in an external media after each operations. This media is stored in an environment with a sufficient security level. These journals allow to ensure the auditability and accountability of the actions (timestamp, person name).

Non-computerized event records are made for:

- production site access;
- maintenance actions and configuration changes;
- human resource changes;
- actions on media with store confidential information.

5.4.2 Frequency of processing log

The event journals are always audited when an abnormal event occurs.

5.4.3 Retention period for audit log

The event journals are externalized every months and stored in a storage server inside UNIVERSIGN premises. They are kept until the expiration of the last certificate issued the CA.

5.4.4 Protection of audit log

The event journal can be accessed only by authorized people of UNIVERSIGN. Each modification must be authorized.

5.4.5 Audit log backup procedures

Audit logs are backups regularly on an external media.

5.4.6 Audit collection system

UNIVERSIGN audit collection systems are internal.

5.4.7 Notification to event-causing subject

Not applicable.

5.4.8 Vulnerability assessments

The UNIVERSIGN CA cannot be accessed through a network and implements the followings measures:

- daily physical access control within the off-line room;
- daily control of the CRL publication;
- monthly backup of the CA events which are then analysed by the System Auditor.

These measures allow the CA to detect:

- unauthorized access;
- technical issues;
- inconsistencies between the different events of the CA.

5.5 Records archival

5.5.1 Types of records archived

The data archived are the following:

- the software and the configuration files of the computer systems;
- the CP and CPS;
- the certificates and the CRLs published;
- the registration files of the SCOs;
- the TSU registration request forms;
- the TSU revocation request forms;
- the audit logs.

5.5.2 Retention period for archive

TSU registration forms:
The TSU registration forms are kept for the whole life of the CA.

Certificates and CRLs issued by the CA:
The TSU and CA certificates, as well as the CRLs, are archived for at least five years after the expiry of these certificates.

Audit logs:
Audit logs are archived and kept 7 years after the expiry of the last certificate issued by the CA.

Archive are held in conformity with applicable legislation (see Sect. 9.4.1) and the obligations of Universign function as CSP (see Sect. 5.8).

5.5.3 Protection of archive

Regardless of their storage media, archives are protected in integrity, and are only accessible by authorized personnel. The archives are readable and usable during their whole life-cycle and are kept in a secure environment.

5.5.4 Archive backup procedures

Not applicable.

5.5.5 Requirements for time-stamping of records

Events shall contain time and date information. Such time information need not be cryptographic-based.

5.5.6 Archive collection system

UNIVERSIGN archive collection systems are internal.

5.5.7 Procedures to obtain and verify archive information

The archives (paper and electronic) can be retrieved in at most two working days. These archives are kept and managed by UNIVERSIGN personnel.

5.6 Key changeover

Universign has no automatic procedure for key changeover. However, at a suitable time before the expiration of a Primary CA signing key, the Primary CA shall generate a new certificate-signing key pair and shall apply all necessary actions to avoid disruption to the operations of any entity that may rely on the CA key. The new Primary CA key shall also be generated and distributed in accordance with this CP.

So, the CA certificate are renewed at most every four years. Since their validity period is ten years, UNIVERSIGN will use several CA certificates and keys at the same time.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

UNIVERSIGN has setup processes and technical means to report and handle incidents (awareness, personnel training, audit log analysis, . . .).

A major incident, a loss, a suspected compromise or a theft of the CA private key for instance, is immediately reported to the CA Approval Board, which, if needed may then decide to terminate the CA.

In all cases, the CA will directly and immediately notify the SGMAP contact point identified of the web site: http://www.modernisation.gouv.fr/.

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

An Activity Continuity Plan has been setup in order to ensure the business continuity of all PKI components. This plan is tested at least once every three years.

5.7.3 Entity private key compromise procedures

The compromise of a key of the CA will lead to the immediate revocation of all issued certificates. In such a case, the various participants will be notified that the CRL may not necessarily be fully trusted. Similar procedures are applied if any of the algorithms, or associated parameters, used by the Primary CA or its TSU become insufficient for its remaining intended usage.

5.7.4 Business continuity capabilities after a disaster

The ability to continue activity after a disaster is described in Universign Disaster Recovery Plan. After a disaster the Primary CA performs this plan to reactivate the stopped services. In particular, each critical service of a Primary CA has a backup service. Moreover, Universign have spare hardware to supply any hardware failure. In case of major disaster, Universign has a recovery plan allowing the setup of a new Primary CA in a reasonable time. This plan is based on a secondary data center, that can host the services in case of necessity.

After the recovery, Universign, when possible, takes new measures to avoid a similar disaster. The recovery operations are made by people in trusted roles.

Disaster Recovery plan is tested every 3 years.

5.8 CA or RA termination

In case of termination of a Primary CA, Universign establishes a termination plan. This plan may include (but is not limited to) the followings:

1. notification of the termination to the SGMAP contact point identified on the web site: http://www.modernisation.gouv.fr;
2. potential revocation of all issued certificate which are still valid;
3. fate of the Primary CA private key, that must be destroyed or put beyond use;
4. necessary undertakings to transfer obligations for maintaining registration information, revocation status information and event log archives for their respective period of time as indicated to the relying parties;
5. publication of the corresponding information for the relying parties.

This plan is checked and updated on a regularly basis.

6 Technical security controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

CA Keys:
Primary CA keys are generated

- during a key ceremony in front of witnesses including a bailiff;
- by personnel in Trusted Role, at least under dual control (see Sect. 5.2.1);
- within secured area (see Sect. 5.1);
- within an HSM that meets the requirements defined in section 6.2.11 and appendix A.

The keys ceremony follows a precise procedure and gives rise to a formal minutes.

TSU Keys:
TSU keys are generated

- within secured area (see Sect. 5.1);
- within an HSM that meets the requirements defined in section 6.2.11 and appendix B.

6.1.2 Private key delivery to subscriber

Not applicable. The TSUs have their own HSMs to generate key pairs.

6.1.3 Public key delivery to certificate issuer

The operation consisting in having the CA sign a TSU certificate is performed on-site by accredited personnel. The TSU public key is delivered on site to the CA.

6.1.4 CA public key delivery to relying parties

The certificate of the UNIVERSIGN CA together with its hash are published on the site: http://docs.universign.eu.

The certificate must contains all the informations described in chapter 7 of this CP.

Relying Parties can also send an email to the contact point identified in section 1.5.2 requesting a confirmation of the CA certificate. The subject of the mail must contain the following information: "Demande du certificat AC UNIVERSIGN ".

6.1.5 Key sizes

The keys used by the UNIVERSIGN CA have the following characteristics:

Certificate	Key Size	Format
UNIVERSIGN CA	2048	RSA
UNIVERSIGN TSU	2048	RSA

6.1.6 Public key parameters generation and quality checking

The key generation material uses parameters fulfilling the security requirements of the algorithm corresponding to the key pair.

The parameters and the algorithms uses are described in section 7 of this CP.

6.1.7 Key usage purposes

Refer to section 7.1.

6.2 Private key protection and cryptographic module engineering controls

6.2.1 Cryptographic module standards and controls

The HSMs used by Universign to generate and use signature keys are certified w.r.t. the requirements of Section 6.2.11. The CA shall ensure the security of HSMs throughout its life cycle.

In particular the CA shall take reasonable steps to ensure that:

- the HSMs are not tampered with during shipment.
- the HSMs are not tampered with during storage before the key ceremony.
- the installation, activation, back-up and recovery of the CA's signing keys in HSMs requires the simultaneous control of at least of two employees in a Trusted Role.
- the HSMs are functioning correctly.
- the CA keys stored in HSMs are destroyed when the device is taken out of service.

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

The CA private key is controlled by activation data stored on smart cards handled to key custodians during the key ceremony.

This activation data is split among the smart cards using the Shamir secret sharing technique.

6.2.3 Private key escrow

Private keys are not escrowed.

6.2.4 Private key backup

CA private keys are backup for recovery purposes, outside of HSMs, but encrypted and with integrity controls.

All private key backups of the CA are stored inside a safe.

The encryption mechanism used provides a security level similar to storage inside the HSM itself, and uses an algorithm, a key length, and a usage mode supposed to resist cryptanalysis for at least the life duration of the protected private key.

6.2.5 Private key archival

The CA and the TSU private keys are not archived.

6.2.6 Private key transfer into or from a cryptographic module

The private keys of the CA are generated inside its HSM and are never transferred except for a backup copy. When the backup copy is generated, the transfer uses an encryption mechanism ensuring that no sensitive information is transferred in a non secure way.

6.2.7 Private key storage on cryptographic module

The private keys of the CA are stored within its HSM.

For recovery purposes, a backup copy is stored outside the module in conformance with 6.2.4.

6.2.8 Method of activating private key

CA private keys:
CA private key activation is controlled by activation data and is performed within an HSM that meets the requirements of appendix A, under dual control of personnel in a Trusted Role.

TSU private keys:
TSU private key activation is controlled by activation data and is performed on an HSM that meets the requirements of appendix B.

6.2.9 Method of deactivating private key

CA private keys:
The private key is deactivated when the HSM stops.

TSU private keys:
The private key is deactivated when the HSM stops.

6.2.10 Method of destroying private key

CA private keys:
CA private key destruction is performed from its HSM. When a key is destroyed, the CA ensures that all corresponding backup copies are also destroyed.

TSU private keys:
TSU private key destruction is performed from its HSM.

6.2.11 Cryptographic Module Rating

CA HSM:
The CA HSM has been:

- Common criteria EAL 4+ ISO/CEI 15408 (Protection Profile: CWA 14167-2 or CWA 14167-3); or
- FIPS 140-2 level 3 or equivalent; and
- qualified at the highest level by the ANSSI (reference 2010/09).

TSU HSM:
The CA does not provide the TSUs. HSM must meet the requirements of appendix B.

6.3 Other aspects of key pair management

6.3.1 Public key archival

The CA public keys are archived for 5 years after the expiry of the corresponding CA certificate.

6.3.2 Certificate operational periods and key pair usage periods

CA:
The CA private keys and certificates have a validity of 10 years.

TSU:
The TSU private key has a validity period of 1 year. The TSU certificate has a validity period of 6 years.

6.4 Activation data

6.4.1 Activation data generation and installation

Generation and installation of the activation date corresponding to the CA private key
The generation and the installation of the activation data of the CA HSM are performed during the key ceremony. These activation data are stored on smart cards and given to key custodians.

6.4.2 Activation data protection

The activation data are stored within nominative and personal smart cards. Each card is under the responsibility of the person it belongs to and is protected by a PIN known only by the card holder. Smart cards are stored in safes when not in use.

6.4.3 Other aspects of activation data

Activation Data Transmission

If a smart card containing activation data is transmitted from one key custodian to another, the transmission is performed using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys.

Activation Data Destruction

Activation data for CA private keys shall be decommissioned using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of the private keys protected by such activation data.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

The Primary CA has appropriate platform-oriented controls in place (such as antivirus, anti malware, ...) to prevent unauthorized or illegitimate software from running within its systems.

Each Primary CA has security controls in place for all accounts with certificate issuance rights. Universign maintains the security level at all time.

These security control mechanisms are described in this chapter.

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 PKI equipments are specified and documented, as well as the registration/de registration 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.

All unauthorized users 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. The administration and operation procedures of the PKI are documented, followed, and regularly updated. The installation controls (initial security configuration of servers) are documented. The end of life controls (destruction) of equipments are documented in order to ensure the non disclosure of sensitive information they may contain.

The set of sensitive hardware of the PKI has maintenance procedures to ensure the availability of the functions and informations. These procedures are documented. Personnel that needs to apply these procedures are appointed by UNIVERSIGN management. Controls of maintenance operations are put in place.

Components integrity
The components of the local network are kept in a physically secure environment. Periodic conformance verifications of their configurations are performed. The vulnerability patchs are deployed, after qualification, within a reasonable period after their publication.

Connection security
Security controls have been setup to ensure the origin authentication, the integrity and when needed the confidentiality of the information exchanged between the different components.

Events and audit
It is possible to trace activity through event logs. That allows especially to notify the appropriate parties in line with the applicable regulatory rules of any breach of security detected.

Supervision and controls
A constant monitoring has been implemented and alarm systems are installed in order to detect record and allow rapid reaction against any unauthorized or abnormal attempt to access resources (physical and/or logical).

Awareness
Awareness procedures of the personnel have been setup.

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 PKI developed by Universign are developed in conditions and following a process that ensures their security. Universign uses

quality process during design and development of their software. Universign ensures, during software updates, the origin and integrity of the software and the traceability of all the modifications applied on the PKI.

Development and testing infrastructures are separated from the production infrastructure of the PKI. Moreover, the test certificates are issued by a dedicated CA whose CN is "Test Universign CA".

6.6.2 Security management controls

Universign ensures that all software updates are done in a secure way. Updates are performed by personnel in Trusted Role.

Universign also ensures that the assets are stored and managed in order to guarantee the confidentiality and integrity of the data.

6.6.3 Life cycle security controls

Not applicable.

6.7 Network security controls

The Universign primary CA is operated offline. Information transmission such as CRL transmission is performed through a mono-directional channel. Thus, this leads to a strict segmentation of its key certificate issuance systems from unrelated servers and systems. Moreover, the criticals components are placed in the securiest areas.

The network communications transferring confidential information are protected against eavesdropping. The rules of the firewalls are checked on regularly basis.

Universign configures all CA systems with the same hardened master (by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the CA's operations).

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

Primary CA maintain access right management procedures to ensure security of the access at a high level. These procedures include administrator authentication, audit log generation, use of secured channels like VPN and availability of access right modification service. Universign also set up a dedicated network for administration purpose.

Primary CA maintains access control procedure to separate administrative and operational practices. All functions (publication, certificate generation, revocation) need an authentication to be executed.

Primary CA maintains an access control policy to limit functions access to authorized people in trusted roles only.

6.8 Time-stamping

The servers of the UNIVERSIGN CA synchronise amongst themselves several times a day with the same time source (UTC). However, the UNIVERSIGN CA is operated off-line ; thus, when a CA operation is performed, a verification of the clock is operated to ensure the PKI servers are correctly synchronized with UTC.

7 Certificate, CRL and OCSP profiles

7.1 Certificate profiles

All certificates issued by Universign comply with X.509, [ETSI EN 319 412-2] and [ETSI EN 319 412-3] standards.

Note : the root and subordinate CAs' certificates comply with the standard [ETSI TS 102 042] until their renewal.

7.1.1 CA certificate

Base fields

Field	Value
Version	2
Serial Number	defined by the tool
Signature	RSA/SHA-256
Issuer DN	C=FR, O=Cryptolog International, OU=0002 43912916400026, CN=Universign Timestamping CA (or Universign Timestamping CA 2015)
Validity	10 years
Subject DN	C=FR, O=Cryptolog International, OU=0002 43912916400026, CN=Universign Timestamping CA (or Universign Timestamping CA 2015)
Public Key	RSA 2048 bits

Certificate extension

Field	OID	Critical	Value
Subject Key Identifier	2.5.29.14	No	
KeyIdentifier			RFC 5280 - Method 1
Key Usage	2.5.29.15	Yes	
digitalSignature			False
nonRepudiation			False
keyEncipherment			False
dataEncipherment			False
keyAgreement			False
keyCertSign			True
cRLSign			True
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	
CA			True
Maximum Path Length			Absent

7.1.2 Certificate of the TSU

Base fields

Field	Value
Version	2
Serial Number	defined by the tool
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, OI=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			0.4.0.2042.1.2
qualifier			http://docs.universign.eu/
Basic Constraint	2.5.29.19	Yes	
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 CRL Profile

Base fields

Field	Value
Version	1
Signature	RSA/SHA-256
Issuer DN	C=FR, O=Cryptolog International, OU=0002 43912916400026, CN=Universign Timestamping CA (or Universign Timestamping CA 2015)
Validity	7 days
Next Update	This Update + 1 day

CRL Extension

Champ	OID	Critical	Value
Authority Key Identifier	2.5.29.35	No	
KeyIdentifier			RFC 5280 - Method 0
CRL Number	2.5.29.20	No	
CRLNumber			defined by the tool

7.3 OCSP Profile

Not Applicable.

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 PKI; or
  - by an internal auditor.
- a [RGS] qualification audit performed by an accredited organization at least every 2 years;
- a [ETSI EN 319 411-1] conformance audit performed by an accredited organization at least every 2 years.

An audit ensuring compliance to this CP shall be performed

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

8.2 Identity/qualifications of assessor

The assessor must act with rigour 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 CA 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 independent from the CA.

8.4 Topics covered by assessment

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

- the CP;
- the CPS;
- the components of the PKI.

Prior to every audit, the assessor will provide the CA 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 CA the result which can be "success", "failure" or "to be confirmed".

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

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

In case of success, the CA confirms that the audited component complies with the requirements of the CP.

8.6 Communication of results

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

9 Other business and legal matters

9.1 Fees

9.1.1 Certificate issuance or renewal fees

Not applicable.

9.1.2 Certificate access fees

Not applicable.

9.1.3 Revocation or status information access fees

Not applicable.

9.1.4 Fees for other services

Not applicable.

9.1.5 Refund policy

Not applicable.

9.2 Financial responsibility

9.2.1 Insurance coverage

Universign subscribes to a professional insurance, allowing in particular to cover all commitments of Universign function as CSP.

Universign encourages (with no obligation) its customers to subscribe to a similar insurance.

9.2.2 Other assets

Universign maintains a financial policy aimed at ensuring, insofar as is possible, it has sufficient financial resources to perform the operations and obligations defined in this CP.

9.2.3 Insurance or warranty coverage for end-entities

Not applicable.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

The following information are classified as confidential:

- private keys of the CA and of the TSUs,
- non-public part of the CPS,
- activation data linked to the private keys of the CA and of the TSUs,
- event journals,
- revocation cause of the certificates.

9.3.2 Information not within the scope of confidential information

Not applicable.

9.3.3 Responsibility to protect confidential information

UNIVERSIGN processes confidential data in respect with the current laws and regulations.

9.4 Privacy of personal information

9.4.1 Privacy plan

UNIVERSIGN gathers and processes the personal data in compliance with the French and European obligations regarding personal data protection.

9.4.2 Information treated as private

Only information concerning the SCO is recorded in the scope of UNIVERSIGN CA.

9.4.3 Information not deemed private

No specific commitments.

9.4.4 Responsibility to protect private information

Not applicable.

9.4.5 Notice and consent to use private information

Not applicable.

9.4.6 Disclosure pursuant to judicial or administrative process

Recordings may be disclosed to be used as legal proof during a legal procedure or requisition of an authorized legal or administrative authority.

9.4.7 Other information disclosure circumstances

No specific commitments.

9.5 Intellectual property rights

Regarding intellectual property, the products operated to provide the PKI 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.

9.6 Representations and warranties

The components of the PKI must ensure to:

- protect the integrity and confidentiality of their secret/private keys;
- use their cryptographic key (public, private and/or secret) only for the usages described during their issuance and with the tools specified in the terms of this CP and its subsequent documents;
- respect and apply their part of the CPS (this part shall be made available to the component);
- submit to the compliance audit performed by the assessment team appointed by UNIVERSIGN CA;
- document their internal processes;
- implement the measures (technical and human) necessary to accomplish its commitments in an environment which guarantees quality and security.

9.6.1 CA representations and warranties

UNIVERSIGN is in charge of:

- validation and publication of the CP;

- validation of the CPS and of their compliance with the CP;
- compliance of the issued certificate with this CP;
- abidance to the security principles for all the components of the PKI and their subsequent controls.

Unless the CA can demonstrate its has not made any intentional or negligence error, the UNIVERSIGN CA is responsible for damages caused to Relying Parties if:

- the informations contained if the certificate does not match the registration informations;
- the CA did not record the revocation of a certificate and did not publish this information in conformance with its commitments.

9.6.2 RA representations and warranties

See above.

9.6.3 Subscriber representations and warranties

The SCO must:

- Communicate correct and up to date information when requesting a TSU certificate;
- Protect the server private under his responsibility;
- Protect the access the the server certificate base;
- Abide by the conditions of use of the server private key according to what is established in this CP;
- Inform the CA of any modification regarding the information contained in the TSU certificate;
- Immediately performs a revocation request of a TSU certificate in case of suspected compromise of the corresponding private key.

The SCO is registered with the CA according to the process defined in this CP.

9.6.4 Relying party representations and warranties

Relying Parties using certificates from the CA must:

- verify and abide by the usage for which the certificate has been issued;
- verify the revocation status of the certificate;
- verify and abide by the obligations defined in this CP.

9.6.5 Representations and warranties of other participants

Not applicable.

9.7 Disclaimers of warranties

Not applicable.

9.8 Limitations of liability

UNIVERSIGN cannot be held liable for non-authorized or non-compliant established in the current CP for the usage of the certificates, the associated private keys and activation data, the CRLs as well as any other hardware of software provided.

UNIVERSIGN cannot be held liable for any damage resulting from errors or inaccuracies of information contained in the certificates, when these errors or inaccuracies are a direct result of erroneous information provided by the Subscriber.

To the extent of the applicable law, the liability of UNIVERSIGN towards the Subscriber or a Relying Party is limited according to what is stated in this CP.

In addition, within the limit set by applicable law, in no event will UNIVERSIGN be liable for:

- Any loss of profits;
- Any loss of data;
- Any indirect damages arising from or in connection with the use of a certificate;
- Any other damages.

In any case, whatever originating facts and prejudices and their aggregate amounts, UNIVERSIGN responsibility will be limited to the amount paid by the Subscriber to UNIVERSIGN regarding the originating fact, with respect to the governing law. Unless otherwise legally enacted, any suit from the Subscriber regarding these CP will take place no longer than six months after the fact originating the legal action.

9.9 Indemnities

UNIVERSIGN is allowed to ask the Subscriber for indemnities if the Subscriber does not respect the agreement with the UNIVERSIGN CA.

9.10 Term and termination

9.10.1 Term

This CP remains in effect until the expiration of the last certificate issued under it.

9.10.2 Termination

This CP shall remain in force until it is replaced by a new version.

9.10.3 Effect of termination and survival

Not applicable.

9.11 Individual notices and communications with participants

Unless otherwise agreed upon by the relevant parties, all notices and other communications to be provided, delivered or sent in compliance with the current CP should be written and sent with means providing reasonable confidence of origin and reception.

9.12 Amendments

9.12.1 Procedure for amendment

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

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

9.12.2 Notification mechanism and period

The only modifications that the Approval Board can perform on the current CP 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 CP will be published for comments, which an indication of the proposed effective date.

When a new version of the CP is published, all the Subscribers and Relying Parties of the UNIVERSIGN PKI are informed of the nature, the time and the date of change, through a publication on UNIVERSIGN web site.

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

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

9.12.3 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 certificates already issued.

9.13 Dispute resolution provisions

Universign set up a procedure for complaint management.

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

9.14 Governing law

See above.

9.15 Compliance with applicable law

This CP complies with the French governing Law, and notable with: [**CNIL**], [**ORD**], [**DRGS**] and [**ARGS**].

9.16 Miscellaneous provisions

9.16.1 Entire agreement

Not applicable.

9.16.2 Assignment

Not applicable.

9.16.3 Severability

Not applicable.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Not applicable.

9.16.5 Force majeure

Are considered force majeure, all the events usually considered as such by French tribunals, notably events that are irresistible, overwhelming and unpredictable.

9.17 Other provisions

9.17.1 Organization reliability

Universign ensures that activities are non-discriminatory.

Moreover, staff in trusted roles is free from any commercial, financial and other pressures which might adversely influence trust in the Universign's services. In particular, employees concerned with certificate generation and revocation management are organized in order to safeguard impartiality of operations.

9.17.2 Accessibility

Universign ensures that services are accessible for persons with disabilities.

A Security requirements on the CA HSM

A.1 Security objectives requirements

The HSM used to generate the certificates and the CRLs must meet the following security requirements:

- Ensuring the confidentiality and the integrity of the CA private signing key during all their life cycle, as well as their safe destruction at the end of the life cycle;
- Being able to identify and authenticate its users;
- Limiting access to its services depending on the user and the role he has been assigned;
- Being able to perform a set of tests to verify it is operating properly and enter a safe state if an error is encountered;
- Allowing the creation of a digital signature to sign certificates generated by the AC, which does not reveal the CA private keys and cannot be forged without the knowledge of the private keys;
- Creating audit logs for every modification regarding security;
- If backup and restore of private keys is provided, ensuring the confidentiality and the integrity of the backup data and require at a minimum dual control of backup and restore operations;
- Detecting physical disruption attempts and enter a safe state when such an attempt is detected.

A.2 Requirements on certification

The HSM used by UNIVERSIGN is qualified at the "reinforced" (in French: renforcé) level, according to the process defined in the [RGS], and complies with the requirements defined above.

B Security requirements on the server HSM

B.1 Security objectives requirements

The HSM used by the server to generate, store and use its key pair must meet the following security requirements:

- Ensuring the key pair generation is performed solely by authorized users and ensuring the cryptographic robustness of the generated key pair;

- Detecting anomalies during initialization, personalization and operation phases and provide safe destruction techniques of the private key;
- Ensuring confidentiality and integrity of the private key;
- Ensuring the link between the private key and the public key;
- Generating a digital signature which cannot be forget without the knowledge of the private key;
- Ensuring digital signature generation for the legitimate server only, and protecting the private key against any usage by third parties;
- Ensuring the authenticity and the integrity of the public key when exported outside the hardware.

References

[**ARGS**] Arrêté du 6 mai 2010 portant approbation du référentiel général de sécurité et précisant les modalités de mise en oeuvre de la procédure de validation des certificats électroniques.

[**DRGS**] Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

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

[**RGS**]
Référentiel Général de Sécurité - Version 1.0 - 06/05/2010.

[**RGS_A_10**]
Référentiel Général de Sécurité - Politique de Certification Type Cachet - Version 2.3 - 11/02/2010. OID: 1.2.250.1.137.2.2.1.2.2.6

[**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

[**RGS_A_14**]
Référentiel Général de Sécurité - Profils de certificats / LCR / OCSP et Algorithmes Cryptographiques - Version 2.3 - 11/02/2010. OID: 1.2.250.1.137.2.2.1.2.1.4

[**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)

[**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.