Universign Hardware CA

Certification Policy
Certification Practice Statement

OID: 1.3.6.1.4.1.15819.5.1.3.(1/3/4/5)

VERSION: *2*	DISTRIBUTION: ***PUBLIC***	Effective date: ***01/07/2016***

Contents

1 Introduction

1.1 Overview

Universign has become a Trust Service Provider issuing public key certificates. For that, Universign operates several Certification authorities. The set of all these certification authorities belongs to the Universign Trusted Network (UTN). In the scope of this UTN, Universign operates Primary Certification Authorities (Primary CAs). Each Primary CA only certifies Subordinate Certification Authority (Subordinate CAs a.k.a Hardware CAs) able to deliver certificates that meet security standards defined or recognised by the European Commission and the French institution ANSSI.

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

This document (hereafter known as CP/CPS in this document) contains both the certification policy of the Hardware CAs and the certification practice statement of the Hardware CAs. This document defines Universign commitments, in terms of security, procedures and requirements regarding the issuance of certificates by the Universign Hardware CAs.

Universign Trusted Network The Universign Trusted Network (presented [1] in Figure 1.) consists of:

- Primary CAs;
- CAs, issuing end holders certificates, linked to at least one Primary CA;
- Certificate's end-holders;
- Relying Parties.

A Primary CA only delivers certificates to CAs that meet the requirements described in their own CP/CPS. The current CP/CPS document only considers CAs that deliver certificates to end-users, which can be physical persons or organisations. Next versions of this CP/CPS may consider CAs delivering certificates for other CAs.

This version of the UTN describes two kind of hierarchy:

- hierarchies with a Hardware Primary CA as Root CA, that aim at issuing hardware end-user certificates and that are called Hardware Hierarchies.

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

- hierarchies with a Software Primary CA as Root CA, that have no hardware protection condition on end-user certificates and that are called Software Hierarchies.

The scope of this CP/CPS focuses on CAs delivering hardware certificates to end-users. End-users may be physical person or organisations.

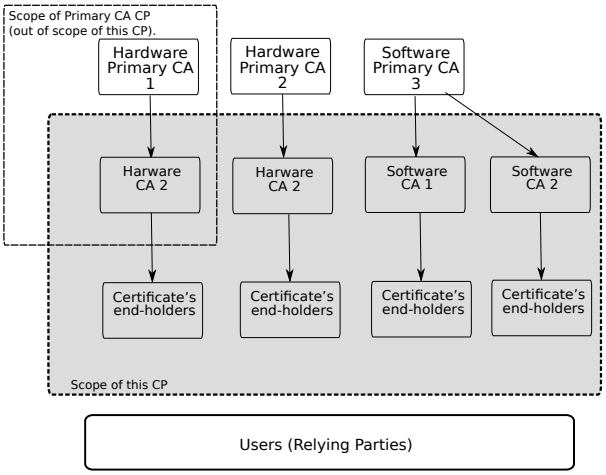

Figure 1: Overview of the Universign Trusted Network and scope of this CP

The current CP/CPS document considers 4 certificates family in conformity with Sections 1.2, 6.2.7 and 7.1.2:

- Physical person certificates, in conformity with [ETSI 319 411-2] QCP-n level, corresponding to the OID 1.3.6.1.4.1.15819.5.1.3.1[2];
- Organization certificates, in conformity with [ETSI 319 411-1] QCP-l level, corresponding to the OID 1.3.6.1.4.1.15819.5.1.3.5[3].
- Physical person certificates, in conformity with [ETSI 319 411-1] LCP level, corresponding to the OID 1.3.6.1.4.1.15819.5.1.3.3;
- Organization certificates, in conformity with [ETSI 319 411-1] LCP level, corresponding to the OID 1.3.6.1.4.1.15819.5.1.3.4.

CP Scope The scope of this CP/CPS is limited to the Hardware CAs and the end-user certificates issuance.

This CP/CPS defines the following Parties:

[2]These certificates are EU qualified certificates and do not require use of a QSCD.
[3]These certificates are EU qualified certificates and do not require use of a QSCD.

- Hardware CAs, with practices in conformity with the requirements of this CP/CPS, delivering certificates to Subscribers,
- Subscribers, that are certificates holders issued by the Hardware CAs;
- users (relying parties) whose operations lean on the trusted architecture provided by Universign.

1.2 Document name and identification

This document is the Certification Policy of the Universign Hardware CAs. It includes also the associated Certification Policy Statement.

Universign, acting as the policy-defining authority, has assigned within the documentation framework of the UTN, an object identifier value extension for each Class of Certificate delivered by its Hardware CA:

- 1.3.6.1.4.1.15819.5.1.3.1 for Hardware CA for individuals (registration with physical presence);
- 1.3.6.1.4.1.15819.5.1.3.5 for Hardware CA for entities or organizations (registration with physical presence);
- 1.3.6.1.4.1.15819.5.1.3.3 for Hardware CA for individuals (registration without physical presence);
- 1.3.6.1.4.1.15819.5.1.3.4 for Hardware CA for entities or organizations (registration without physical presence);

1.3 PKI participants

1.3.1 Certification Authorities

A certification authority is an umbrella term designing an authority that can issues certificates to certificate's holders.

Within the Universign Trusted Network, two kinds of entities correspond to that generic description:

- the Primary CAs, that issue certificates for Hardware CAs.
- the Hardware CAs, that issue certificates for end-user Subscribers (see Section 1.3.3).

The perimeter of this CP/CPS focuses on the Hardware CAs and the issuance of certificates to the Subscribers (see Section 1.1).

Hardware CA Management 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 Approval Board has the final authority and responsibility for:

- specifying and approving the Hardware CA documentation corpus.
- approving the CP/CPS;
- defining the update process of the CP/CPS, with the responsibility of the maintenance of the CP/CPS;
- defining the review process ensuring that Universign correctly abides by the practices defined in the CP/CPS;
- publishing the CP/CPS, as well as their revisions, to Subscribers and Relying Parties.

1.3.2 Registration Authorities

In the scope of this CP/CPS, Universign Hardware CA operates its own Registration Authority. The Hardware CA may delegate some Registration operations to Third Parties under contract with Universign. In this case, Universign performs a second check of the data received by the Third Parties.

1.3.3 Certificate's Holders

Certificate's holder is a generic name that may refer to the following entities:

- The Subject, that can be either a physical person, a legal person, an organization, an entity, a component or an infrastructure and that is defined by the `subject` field of the certificate;
- The Subscriber, that can be a physical person or an organization that subscribes with the certificate issuer. Notice that the Subscriber and the Subject may be different: an organization may subscribe with a CA for issuing certificates to its employees;
- The Certificate's owner, that refer to the person that is responsible for the Certificate's life cycle (certificate request, revocation,...).

Depending on the architecture, the above people and entities may be merged or may be different.

In this CP/CPS, we have 2 kinds of certificates:

- Physical person certificates;
- Legal person certificates

Therefore, in this CP/CPS,

- The Subject must be either [4]:
  - A physical person (in association with an organisation or not); or
  - A entity or organization.

  The Subject is defined within the `subject` field of the certificate issued by the CA.
- The Certificate holder is:
  - The subject itself, when the subject is a physical person;
  - A *Certificate Owner* , named by the Subscriber (See Section 1.3.5), when the Subject is a entity or an organization. This Certificate Owner is responsible for the certificate's life cycle operations.

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 Universign Hardware CA, particularly the association between the Subject and the public key. A Relying Party is responsible for deciding how to check the validity of a Subject 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

In the case of issuance of a certificate to an organization or entity, Universign defnies also :

[4] next versions of this CP/CPS may consider other classes of subjects, such as CA, components or infrastructures

Certification Representative Certification Representative may only be named in the case of certificates issued to organizations. In that case, Certification Representatives must be formally named by a legal representative of the organization. The Certification Representative is directly in contact with the Hardware CA Registration Authority.

The role of the Certification Representative is defined as follow:

- The Certification Representative must correctly and independently perform the identity check of the future Subjects of the organization he or she represents.
- The Certification Representative must respect the practices described in this CP/CPS.

If a Certificate Representative is leaving the organization, the organization contracting with the CA is responsible:

- for noticing the Hardware CA prior to the departure, or at least within the best delay;
- for naming a new Certification Representative

Certificate Owner Certificate Owner must be a physical person responsible:

- for handling administrative tasks related to the organization or entity certificate issuance, and the life cycle of the certificate;
- of the private key associated to the certificate.

The Certificate Owner shall be authorized for handling these responsibilities for the organization referred within the certificate. Therefore, the Certificate Owner must have a contractual, hierarchical or regulatory relation with the organisation and must be explicitly named by the organization. The Certificate Owner shall respect all the role-related requirements defined in this CP/CPS.

It is important to notice that organization or entity certificates are not attached to a physical person, therefore, the Certificate Owner may change before the expiration of the certificate, for example, when the Certificate Owner is leaving the organization or when the Certificate Owner has a new assignment within the organization. The organization must notice the Hardware CA prior to the change or immediately after the change and name a new Certificate Owner. A Hardware CA shall revoke the organization Certificate if no Certificate Owner is named after several notification to the organization.

1.4 Certificate Usage

1.4.1 Appropriate certificate uses

Certificates issued by the Hardware CA The key pair associated to certificates issued by the Hardware CA are used to electronically sign data in the scope of electronic exchange between end-users with certificates.

Hardware CA Certificate and Key Pair The Hardware CA has only one key pair. This key pair is certified by a Primary Hardware CA. This key pair is used to sign:

- end-users certificates;
- its CRLs and/or its OCSP responses;
- technical certificates of the components of its infrastructure.

1.4.2 Prohibited certificate uses

Any usage other than those defined in the previous paragraph is prohibited by this CP. Certificates shall be used only to the extent that the use is consistent with applicable law.

1.5 Policy administration

1.5.1 Organization administering the document

Universign
5-7, Rue du Faubourg Poissonnière, 75009 Paris, France
contact@universign.eu

1.5.2 Contact person

Questions concerning this policy should be sent to:

Universign
Hardware CA
For the attention of the Policies Manager
5-7, Rue du Faubourg Poissonnière, 75009 Paris, France
contact@universign.eu

1.5.3 Entity determining the compliance of the practices of the CP

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

1.5.4 CP approval procedures

The approval and maintenance of the conformance of the documented practices with the CP/CPS is pronounced by the Universign Approval Board, in 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/CPS, 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.

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

CPS: Certification Practice Statement

CRL: Certificate Revocation List

DN: Distinguished Name

HSM: Hardware Security Module

OID: Object Identifier

PKI: Public-Key Infrastructure

RA: Registration Authority

RGS: Référentiel Général de Sécurité

TSP: Trusted Services Provider

2 Publication and repository responsibilities

2.1 Repositories

Universign, as Hardware CA, publishes this CP/CPS, making it available for the certificates users. This is available on the Internet, on the website : http://docs.universign.eu.

Public information relative to certification practice are included in this CP/CPS.

2.2 Publication of certification information

The Hardware CA published information is the following:

- this CP/CPS[5];
- the applicable CRLs, in accordance with the Requirements of this CP/CPS;
- the OCSPs certificates;
- CRLs of OCSP server certificates;
- the active certificates of the Universign Hardware CAs .
- the PKI Disclosure Agreement;
- the Subscriber Agreement;
- the Relying Parties Agreement;
- The Terms and Conditions.

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

2.3 Time or frequency of publication

This CP/CPS: This CP/CPS is published in conformity with section 9.12.

CRL: Universign Hardware CAs publish CRLs allowing Relying Parties to check the status of the issued certificates. CRLs are published every day on a publicly available website (see Sect. 2.1).

OCSP certificates: OCSP certificates are included in all OCSP answers. Therefore, they may not be published on the repository.

Universign Hardware CAs valid certificates : Hardware CA certificates are published at least 24 hours after generation and prior to their first use.

The Subscriber Agreement, Terms and Conditions, the PKI Disclosure Agreement and the Relying Parties Agreement are published when necessary after any update.

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

2.4 Access Controls on repositories

Universign shall not intentionally use technical means of limiting access to published information. Persons shall agree to the Relying Parties Agreement prior to accessing the published information.
Universign implements controls to prevent unauthorized persons from adding, deleting, or modifying repository entries.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of names

Names used comply with the requirements of the X.500 norm.

The Hardware CA and Subscriber are identified by an explicit name (called "DN" hereafter) of type X.501. This type of DN is defined in chapter 7. The details of the identification process of a Subscriber by the Universign Hardware CA are described in chapter 3.2.2 and chapter 3.2.3.

Certificates issued to Physical Person All certificates issued by Universign Hardware CA to physical persons contains the following fields in the DN:

Field	Mandatory	Semantics	Verified by the RA	Document used for verification
C	Yes	Nationality of the physical person	Yes	Valid ID document
givenName	Yes	Last name of the physical person	Yes	Valid ID document
surname	Yes	First name of the physical person	Yes	Valid ID document
O	No	Legal name of the entity attached to the physical person	Yes	Valid and legal organization Identification document and Authorization Form
OI	No	Unique identification number of the organization[6] structured in accordance with ISO 6523	Yes	Valid and legal organization Identification document
SERIALNUMBER	Yes	serial number generated by the RA	Yes [7]	
CN	Yes	Last Name and First Name used by the physical person	Yes	Valid ID document

Each DN shall be unique. A unique serial number (field SERIALNUMBER) is included in each certificat to obtain this unicity.

Certificates issued to Entities and Organizations All certificates issued by Hardware CA to Entities and Organizations contains the following fields within the DN:

[6]For a french company, 0002 followed by one space and the SIRET or SIREN number
[7]It will be checked that this number is unique.

Field	Mandatory	Semantics	Verified by the RA	Document used for verification
C	Yes	Country	Yes	Valid Organization Identification document
ST	No	State of the Subscriber	Yes	Valid and legal organization Identification document
L	No	City of the Subscriber	Yes	Valid and legal organization Identification document
O	Yes	Legal name of the Subscriber	Yes	Valid and legal organization Identification document
OI	Yes	Unique identification number of the organization.[8] in conformity with ISO 6523	Yes	Valid and legal organization Identification document
CN	Yes	Free field referring to the organization	Yes [9]	

Each issued DN shall be unique. This unicity is obtained by the unique organization number (field OI).

3.1.2 Need for names to be meaningful

The DN of the Universign Hardware CA is specified in chapter 7. Universign Hardware CA only issues certificate if the DN is meaningfull, *i.e.*, if it allows to determine the identity of the individual or the organization that is the Subject of the Certificate.

3.1.3 Anonymity or pseudonymity of subscribers

These practices are not allowed.

3.1.4 Rules for interpreting various name forms

The interpretation rules are defined in section 7.

3.1.5 Uniqueness of names

The Subject identity (refer to 3.1.1) is unique for all certificates generated by the Hardware CA. The RA ensures this uniqueness through its registration process

[8] For a french company, 0002 followed by the SIRET or SIREN number

[9] It will only be checked that the name is meaningful (seeSect. 3.1.2)

(refer to 3.2.2).

For a certificate of physical person, this is done thanks to a unique serial number within the SERIALNUMBER field of the certificate. For a certificate of organization or entity, this is done thanks to a unique legal number of the organization (typically a SIRET number for a french company) within the OU field of the certificate, and by checking that, for a given organization, the CN field is unique.

3.1.6 Recognition, authentication, and role of trademarks

Certificate Applicants shall not use names in their Certificate Applications that infringe upon the Intellectual Property Rights of others. Neither Universign nor any Affiliate shall be required to determine whether a Certificate Applicant has Intellectual Property Rights in the name appearing in a Certificate Application or to arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any domain name, trade name, trademark, or service mark, and Universign and any Affiliate shall be entitled, without liability to any Certificate Applicant, to reject or suspend any Certificate Application because of such dispute.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

At the time of the certificate application, the Hardware CA requires applicants to provide proof of possession of the private key corresponding to the public key to be certified.

The proof of possession is verified

- either by signing the PKCS#10 certificate request (or mechanism providing equivalent guarantee accepted by Universign) with the Subscriber private key;
- or by requesting from a reputed key service accepted by Universign.

3.2.2 Authentication of organization identity

The validation of identity of an organization is done

- where necessary, for a certificate of physical person in association with an organization :
  - either directly during the registration of the physical person claiming that he is part of the organization;

  - or indirectly during the validation of the identity of the Certification Representative in association with the organization [10];

- for a certificate of organization, during the registration of the Certificate Owner[11].

3.2.3 Authentication of individual identity

Whatever the type of issued certificate, the future Certificate Holder shall provide the necessary evidences of its identity and the elements to be included in the certificate. Universign only requires the elements needed to issue the certificate. A copy of each of these elements has to be included in the registration record and will be kept safe by Universign.

Certificate issued to physical person The ID of the subject is verified by the RA. This verification is done:

- during a face-to-face meeting for certificates issued with OID 1.3.6.1.4.1.15819.5.1.3.1.
- with or without a face-to-face meeting for certificates issued with OID 1.3.6.1.4.1.15819.5.1.3.3.

The applicant shall provide the following elements:

- Official ID document including a recent picture, the place and date of birth of the subject;
- an email address and/or a mobile phone number allowing the Hardware CA to contact the Certificate's Holder.

if the Subject would like to have the certificate associated with an entity or an organization, (*i.e.* having the name of the entity within the `O` field of the certificate and the identification number within the `OI` field), he shall provide the evidence that he is in association with the entity. The requester shall provide the following elements:

- Official ID document including a recent picture, the place and date of birth of a legal representative of the organization;
- An official, valid and legal document that provides evidence of the existence of the organization at time of request (for example, a Kbis document dated within 3 months for a french company). This document shall include a

[10] This point is justified by the fact that there is a limited number of representatives at a given time.

[11] This point is justified by the fact that there is only one Certificate Owner at a given time.

legally recognized unique identification number of the organization (such as a SIRET number for a French company);

- an evidence that the Subject is in association with the entity. This can be done
  - Either with a document signed by a legal representative of the entity, certifying that the certificate requester belongs to the organization and that he is authorized to add the reference to the organization within his certificate. This document shall be dated within 3 months. The document shall be signed by the requester for acceptation.
  - Or by a registration *via* the Certification Representative of the entity or organization. Then, the Certification Representative shall check by its own means that the requester belongs to the organization and certifies of the belonging. The `O` field and the `OU` field (if applicable) are those used during the Certification Representive Registration.
  - Or by other means accepted by Universign that provides sufficient evidence that the requester belongs to the organization and is authorized to use the reference to the organization within its certificate.

Entity or Organization Certificate Identity of the entity or organization Certificate's Holder is checked by the RA.

- during a face-to-face meeting for certificates issued with OID 1.3.6.1.4.1.15819.5.1.3.5.
- with or without a face-to-face meeting for certificates issued with OID 1.3.6.1.4.1.15819.5.1.3.4.

The requester shall provide the following elements:

- Official ID document including a recent picture, the place and date of birth of the Certificate's Holder;
- an email address and/or a mobile phone number allowing the Hardware CA to contact the Certificate's Holder.
- a document signed by a legal representative of the entity, naming the requester as Certificate Holder. This document shall be dated within 3 months and be signed by the requester for acceptation.
- An official, valid and legal document that provide evidence of the existence of the organization at time of request (for example, a Kbis document dated within 3 months for a french company). This document shall include a legally recognized unique identification number of the organization (such as a SIRET number for a French company).

Certification Representative Identification The registration as a Certification Representative require the check of the identity realized during a face-to-face meeting. For the registration as a Certification Representative, the requester shall provide:

- an official ID document including a recent picture, the place and date of birth;
- a document signed by a legal representative of the entity, naming explicitly the requester as Certification Representative of the enity. This document shall be dated within 3 months and this document shall be signed by the requester for acceptation.
- An official, valid and legal document that provide evidence of the existence of the organization at time of request (for example, a Kbis document dated within 3 months for a french company). This document shall include a legally recognized unique identification number of the organization (such as a SIRET number for a French company).

3.2.4 Non-verified subscriber information

No verification is performed on fields that are not explicitly flagged as verified in the section 3.1.1.

3.2.5 Validation of authority

The RA of a Hardware CA validates that the person has the authority to represent the organization with a mandate signed by the legal representative of the organization, as described in Section 3.2.3.

3.2.6 Criteria for interoperation

Not applicable.

3.3 Identification and authentication for re-key requests

The Hardware CA Universign 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

Certificates for physical person Revocation requests can be performed as follow:

- through Universign revocation user interface, after authentication of the user;
- where the user has lost its authentication mean, through a specific service available to all certificate holders. Universign authenticates the user and, on authentication success, revokes the certificate.
- by sending a revocation request by email to the following adress: revocation@universign.eu. A Universign employee having a Trusted Role will then contact directly the requester in the aim of authenticating him or her with the means at his disposal.

Certificate for Entity or Organisation A revocation request is performed by sending an email to the following adress: revocation@universign.eu. The user is contacted back by a Universign employee having a Trusted Role. The Universign employee having a Trusted Role executes a user authentication procedure, based on the elements of the RA record.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate application

4.1.1 Who can submit a certificate application

The requester performs the certificate request by filling the Subscriber registration request form.

4.1.2 Enrollment process and responsibilities

Certificat for physical person, entity or organisation.

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

- The requester shall read and shall accept the the Subscriber Agreement of the Hardware CA.
- the Certificate Holder shall complete a Certificate Application Form filled with correct information. The Certificate Owner shall provide all elements of the registration record, defined in Section 3.2.3, to the RA, or, if applicable, to the Certification Representative;
- The RA or the Certification Representative check the elements provided within the registration request (see Section 3.2.3) and transfers the request to the Hardware CA.
- When registering through a Certification Representative, the registration request is checked again by the RA. If the request is shown to be invalid or incomplete, the Hardware CA revokes the certificate. If the request is valid, the certificate is validated;
- The Subscriber shall generate its own keypair within a hardware cryptographic device satisfying requirements of Section 6.2.11.
- The requester shall provide the public key to the Hardware CA;
- The request shall provide evidence that he owns the private key associated with the public key, in conformity with requirements of Section 3.2.1.

Universign ensures that the registration process is performed within applicable laws.

Registration of a Certification Representative
The registration process of a Certification Representative is the following:

- The organization of the future certification representative shall be under contract with Universign;
- The requester shall send a registration request to the RA and shall provide all the needed elements required in Section 3.2.3;
- The RA checks the request and add the new Certification Representative to its Certification Representative list.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Universign Hardware CA handles the RA function itself. The RA validates Certification Requests of the candidates. The RA performs identification and validation of all required information provided by candidates in conformance with section 3.2.

4.2.2 Approval or rejection of certificate applications

The certificate request validation procedure by a RA is the following:

- the RA, or the Certification Representative, checks that the registration information are complete and valid. Particularly, the RA or Certification Representative checks the conformity of information within the certificate request w.r.t. the evidence provided by the requester.
- the RA, or the Certification Representative performs successfully the requester identification and the identification of information provided in conformity with section 3.2;

If the request is rejected during one of these steps, the requester is immediately informed.

4.2.3 Time to process certificate applications

The Hardware CA processes certificate applications without delay after time of receipt. A certificate application remains active until rejected.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

A Hardware 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.

The public key of the Subject shall by given to the Hardware CA in a secured way.

4.3.2 Notification to subscriber by the CA of issuance of certificate

Universign notifies within a reasonnable delay the Requester that the certificate has been issued. This certificate is transmitted to the Requester in an appropriate way.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The followings are considered as implicit acceptation by a Subscriber of a certificate issued by the Hardware CA:

- download of the certificate by the Subscriber or download of a message containing the certificate;
- no objection of the content of the certificate received in a 48 hours delay after its issuance.

4.4.2 Publication of the certificate by the CA

A Hardware CA does not publish the issued certificates without explicit authorization of the Subscriber.

4.4.3 Notification of certificate issuance by the CA to other entities

Not applicable.

4.5 Key pair and certificate usage

Subscriber:

The certificate shall be used in conformity with:

- Requirements of the CP/CPS, in particular usages defined in section 1.4;
- the Subscriber Agreement;
- all extra conditions defined in the contract between the Hardware CA and the Subscriber, if applicable;
- the `KeyUsage` extension defined in certificate or any extension within the certificate that constrains the key usage.

A Subscriber shall:

- protect its private keys in a cryptographic device in conformity with Section 6.2.11;
- if its private keys are compromised, the use of the Subscriber private key is immediately and permanently discontinued and the fact of this compromised shall immediately be notified to the issuing Hardware CA;
- if the private key of the Hardware CA that issued the certificate has been compromised, the Subscriber shall no longer use its certificate.

Relying Parties:

Relying Parties must accept the Relying Parties Agreement before any use of certificate issued by a Hardware CA. Relying Parties are responsible for:

- determining that certificate use is in conformity with authorised and forbidden use defined in this CP/CPS (see Section 1.4);
- determining that certificate are used in conformity with its `KeyUsage` extension;
- checking certificate status.

4.6 Certificate renewal

Certificate renewal is not allowed by the Hardware CA Universign.

4.6.1 Circumstances 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 renewed certificate

Not applicable.

4.6.6 Publication of the renewed 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 Hardware CA Universign.

4.7.1 Circumstances 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 its revocation followed by a new initial certificate request.

4.8.1 Circumstances 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 certificate issued by Hardware CA the are the following:

- the Hardware CA receives a revocation request from the Subscriber;

- a Subscriber does not respect or has not respected its obligations regarding the Hardware CA, in particular the requirements defined in the Subscriber Agreement;
- the information regarding a Subscriber included in the certificate are no longer accurate;
- Hardware CA or Subscriber strongly suspects the loss or theft of a private key, or that it has been compromised;
- error in the registration procedure;
- if applicable, no payment for the certificate issuance;
- definitive end of activity of a Hardware CA;
- a Subscriber lost control of its private key, due for example to the loss or theft of the activation data of the private key;
- Universign considers that the use of the certificate is harmful.

4.9.2 Who can request revocation

Certificate for physical person People allowed to request a certificate revokation are the following:

- Hardware CA Chief Officer, or when he or she is not available and in case of emergency Universign Approval Board;
- the Subscriber;
- the Subject, if different that the Subscriber.

Certificate for entity or organisation The person who can request revocation of a entity or organisation certificate certificate are:

- Hardware CA Chief Officer, or when he or she is not available and in case of emergency Universign Approval Board;
- the Certificate Owner;
- the legal representative of the entity or organisation.

4.9.3 Procedure for revocation request

The Requester transmits a revocation request which contains at minimum the following information:

- complete name;
- Subscriber identification (see Sect. 3.1.1);
- information allowing the CA to identify the certificate to be revoked (such as Serial number of the certificate or complete DN of the certificate);
- possibly the reason for revocation. This reason is for information purposes and is not listed in the CRL.

Certificate for physical person As defined in Section 3.4, revocation can be done by three ways:

- via the user interface of the service;
- via a specific service, available to any certificate holder;
- via email.

Certificate for entity or organisation The request is sent by email, as explained in section 3.4.

The Universign Hardware CA authenticates the revocation request in accordance with Section 3.4 and revokes the certificate using its key pair. All the operations are protected in a manner to guarantee the integrity, confidentiality (when it is necessary) and origin of transmitted data.

The Universign Hardware CA informes the Subscriber of the revoked certificate and the Requester (if they are not the same person) of the change of status of its certificate. Revocations are definitive.

4.9.4 Revocation request grace period

The revocation request must be submitted as soon possible.

4.9.5 Time within which CA must process the revocation request

The maximum handling period is 24 hours, from acceptance of the request and authentication of the requester, 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

CRLs are issued at least every 60 minutes.

4.9.8 Maximum latency for CRLs

CRLs are published at most 30 minutes after their generation.

4.9.9 Availability of an online revocation/status checking system

Revocation service and certificates status are available on the repository. Information status service includes one or more OCSPs. Universign provides on its repository a link to OCSPs, that can be used to check certificates status. Under normal conditions, OCSPs are available 24/7.

4.9.10 Online revocation checking requirements

Users shall check the status of a certificate before using it to check an electronic signature. Users shall check the certificate against the latest published CRL, or send a status request to an OCSP.

4.9.11 Other forms of information about revocations available

Not applicable.

4.9.12 Special requirements regarding key compromise

Universign notifies all the ACU parties in case of Hardware CA private key compromise or suspicion of private key compromise.

4.9.13 Circumstances for suspension

Certificate suspension is not authorized by this CP/CPS.

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 and web-links to OCSPs are posted on a publication site freely accessible

- from the address defined in Section 2.1;
- from the specific adress defined in the issued certificates.

Universign ensures integrity and authenticity of published CRLs and OCSP's answers. CRLs and OCSP's answers include information on the status of certificates at least until the certificate expires. The qualified certificates are included beyond their expiration.

4.10.2 Service availability

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

4.10.3 Optional features

Not applicable.

4.11 End of subscription

The end of subscription between a Hardware CA and a Subscriber falls under the scope of the contract between a Hardware CA and a Subscriber, which can define obligations that are still valid after certificate revocation or expiration. Without specific clause, the relation expires at the end of the length validity of the certificate or its revocation.

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 (ISP). It describes the approach and the solutions to set up to manage the security.

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

5.1 Physical controls

5.1.1 Site location and construction

Universign hosts its Hardware CA in secured premises. The site location and construction, combined with other physical security protection mechanisms described hereafter, provides robust protection against unauthorized access to the Hardware 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 of the Primary CA are physically isolated from other components.

5.1.2 Physical access

Access to Hardware CA facilities is strictly restricted to authorized personnel listed on an access list. A logbook is updated each time maintenance is operated on the Hardware 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 access cards.

The access security is strengthened by a biometric reader.

Access profiles to each zone are defined and maintained by the Universign.

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 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 exposure

The specification of the security perimeter takes into account the risks related to water exposures. Protection controls are operated 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 These measures meet all local applicable safety regulations.

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 Hardware CA in secured locked premises and stored in a safe which opening means are known only by the Hardware CA Chief Officer and authorized personnel.

Hardware CAs ensure protection against obsolescence and deterioration of media within the period of time that records are required to be retained.

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 Hardware 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 additionnaly approve 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.

RA operator: all registration operation of the new certificates holders.

Hardware CA personal in Trusted Role (and more generally, all Hardware 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 Hardware 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 Hardware 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, ...

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.

5.2.4 Roles requiring separation of duties

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

Every Hardware CA ensures that security operations are separated from standard operating 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 Hardware CAs. This risk analysis is periodically reviewed and each time a structural change occurs on a Hardware CA. 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

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. Trusted Role are appointed by Universign management, the only exception is the registration operators, that are appointed by their organisation.

5.3.2 Background check procedures

Universign (or the third party employing the registration operators) 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 (or the third party employing the registration operators) 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

All personnel is trained on software and hardware in use and on 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 and/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

Subcontractors cannot have a Trusted Role within a Hardware CA , except as registration operator.

Requirements towards subcontractors are subject to contracts.

The contracts established with subcontractors include commitments regarding non-disclosure, security and measures about use of IT assets.

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 Approval Board.

5.4 Audit logging procedures

5.4.1 Types of events recorded

Universign ensures that the following events are recorded:

- all registration events (certificate application);
- all Hardware CAs key life cycle events;
- all life cycle events of certificates issued by Hardware CAs, including revocation events;
- all events from the components of the PKI (servers start or shutdown, network access, ...).

These logs ensure the auditability and accountability of the actions (timestamp, person name), especially on legal request.

The specific events and data to be logged are documented in the CA internal procedures.

The Hardware CA ensures robust logging procedures, including aggregation of logs at alternate sites, tamper evidence controls, and monitoring schedules.

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

On-site retention of event journals is at least a month. The event journals are externalized every month and stored inside Universign premises for a duration needed by proof provision on legal request.

5.4.4 Protection of audit log

The event journal can be accessed only by authorized people from Universign. Each modification must be authorized.

5.4.5 Audit log backup procedures

Audit logs are backups regularly on an external system.

5.4.6 Audit collection system

Universign audit collection systems are internal.

5.4.7 Notification to event-causing subject

No notification are performed

5.4.8 Vulnerability assessments

Universign Hardware CAs implements the followings measures:

- daily physical access control within the production room;
- daily control of the CRL publication;
- daily analysis of CA events by person in Trusted Role;

- regularly security tests (vulnerability scans, penetration tests) and reports.

These measures allow the CA to detect:

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

5.5 Archival of records

5.5.1 Types of records archived

The data archived are the following:

- the registration files of the Subscribers and the Subscribing Entity representatives;:
  - evidence that the the Subscriber Agreement has been accepted by the Subscribers (see Section 4.1.2);
  - the Subscriber registration request forms (see Section 4.1.2);
  - copy of all evidence used to verify a physical person Identity (see Section 3.2.3);
  - if applicable, for physical person certificates linked to an entity or organisation, copy of evidences used to check the link between the physical person and the organization and copy of the evidence of the existence of the organization (see Section 3.2.2);
  - if applicable, for entity and organization certificates, copy of elements used to check the link between the Certificate Owner and the entity or organization, and copy of the evidence of the existence of the organization (see Section 3.2.2);
- the audit logs. In particular:
  - significant Hardware CA enviromental change events and their precise time;
  - key management and certificate management events and their precise time.

Events and data to be logged are documented in the Hardware CA internal procedures.

5.5.2 Retention period for archive

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

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 archives

Regardless of their storage media, archives are protected in integrity, and are only accessible to 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

Regular back-ups of Universign's electronic archives of issued Certificate information are performed. These back-ups are exported to a remote site and are protected in integrity and confidentiality.

5.5.5 Requirements for timestamping 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 Hardware CA signing key, the Hardware 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 Hardware

CA key. The new Hardware CA key shall also be generated and distributed in accordance with this CP/CPS.

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, ...). By this way, Hardware CAs minimizes damages in case of incident.

Hardware CA has set an incident response plan to respond to compromise or breach of its online systems as well as its certificate issuance systems.

A major incident, a loss, a suspected compromise or a theft of the Hardware CA private key for instance, is immediatly reported to the Hardware CA Approval Board, which, if needed may the decide to request the revocation of the certificate Hardware CA to its superior level CAs and to terminate the Hardware CA.

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.

5.7.3 Entity private key compromise procedures

This point is covered by business continuity and business recovery plan. The compromise of a key of the Hardware 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 procedure are applied if any of the algorithms, or associated parameters, used by the CA or its subscribers 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 Hardware CA performs this plan to reactivate the stopped services. In particular, each critical service of a Hardware CA has a backup service. Moreover, Universign have spare hardware to supply any hardware failure. In cas of major disaster, Universign has a recovery plan allowing the setup of a new Hardware CA in a reasonnable 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.

5.8 CA or RA termination

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

1. notification of the termination to all subscribers and other entities with which the Hardware CA has agreements (in particular to forbid the process of all new registration requests);
2. Notification of the termination to all CAs of upper level;
3. potential revocation of all issued certificate which are still valid;
4. fate of the Hardware CA private key, that must be destroyed or put beyond use;
5. 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 Subscribers and relying party;
6. 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

Hardware CA Keys:
Hardware CA keys are generated

- during a key ceremony in front of witnesses including a bailiff;
- by personne 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.

The keys ceremony follows a precise procedure (called key ceremony) and gives rise to a formal minutes.

Subscriber Keys:
Subscriber keys are generated

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

6.1.2 Private key delivery to subscriber

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

6.1.3 Public key delivery to certificate issuer

The Subscriber public key is delivered by the Subscriber to the Hardware CA in an electronic way by a method ensuring its integrity and its origin.

6.1.4 CA public key delivery to relying parties

Universign Hardware CAs certificates are published on the site: http://docs.universign.eu.

The certificates must contain all the informations described in the issuing CA Certification Policy.

Relying Parties can also send an email to the contact point identified in section 1.5.2 to request a confirmation of the Hardware CA certificates. The subject of the mail must contain the following information: "Universign Hardware CA Certificate Request".

6.1.5 Key sizes

The keys used by the Universign Hardware CA have the following characteristics:

Certificate	Key Size	Format
Hardware CA	2048	RSA

The keys used by the Subscribers have the following characteristics:

Certificate	Key Size	Format
Subscriber	2048	RSA

6.1.6 Public key parameters generation and quality checking

The key generation material and algorithmes (voir Sect. 6.2.11) 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 Hardware CA shall ensure the security of HSMs throughout its lifecycle.

In particular the Hardware 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 Hardware CA keys stored in HSMs are destroyed when the device is taken out of service.

6.2.2 Private key control

Hardware CA Keys:
The Hardware CAs' private keys are controled by multiple persons with activation data stored on smartcards that are handed over to the key custodians during the key ceremony.

This activation data is split among the smartcards using a secret sharing technique.

Subscriber Keys:
The Subscriber private keys are controled by activation data under the sole control of the Subscriber.

6.2.3 Private key escrow

Private keys are not escrowed.

6.2.4 Private key backup

Hardware CA private keys are backuped for recovery purposes either:

- outside of HSMs, but encrypted and with integrity controls.The encryption mecanism 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. All private key backups of the Hardware CA are stored inside a safe only accessible by persons in Trusted Role.
- within a HSMs with equivalent or greater security level. The HSMs is operated in equivalent or greater security conditions

Backup are done by a least two persons in Trusted Role.

6.2.5 Private key archival

The Hardware CA private keys are not archived.

6.2.6 Private key transfer to or from a cryptographic module

The private keys of the Hardware CA are generated inside its HSM and are never transferred except for a backup copy (See Section 6.2.4). When the backup copy is generated, the transfer uses an encryption mecanism ensuring that no sensitive information is transferred in a non secure way. Every keys backup and restoration are performed by at least two persons in Trusted Role within secured areas.

6.2.7 Private key storage in a cryptographic module

The private keys of the Hardware CAs and Subscribers are protected by the HSMs.

For recovery purposes, a backup copy of the private keys of the Hardware CAs is stored outside of the module in accordance with 6.2.4.

6.2.8 Method of activating private keys

Hardware CA private key activation is controlled by activation data and is performed within an HSM that meets the requirements of Section 6.2.11, under dual control of personnel in a Trusted Role.

6.2.9 Method of deactivating private keys

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

6.2.10 Method of destroying private keys

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

6.2.11 Cryptographic Module Rating

Hardware CA HSM: The HSM used by the Hardware CA meets the following requirements:

- Common criteria EAL 4+ ISO/CEI 15408 (Protection Profile: CWA 14167-2 or CWA 14167-3); or
- FIPS 140-2 level 3 or equivalent.

Subscriber HSM: The Hardware CA does not provide the Subscribers' HSMs. Subscribers' HSM must meet the following requirements:

- Common criteria EAL 4+ ISO/CEI 15408 (Protection Profile: CWA 14169; or Certification as a Secure Signature Creation Device (SSCD) from an EU government entity); or
- FIPS 140-2 level 3 or equivalent.

6.3 Other aspects of key pair management

6.3.1 Public key archival

The Hardware CA shall archive their own public keys, in conformance with Section 5.5.

6.3.2 Certificate operational periods and key pair usage periods

A Hardware CA shall not issue Certificates to Subscribers if their Operational Periods would extend beyond the validity of the key pair of the Hardware CA.

6.4 Activation data

6.4.1 Activation data generation and installation

Generation and installation of the activation date corresponding to the Hardware CA private key
The generation and the installation of the activation data of the Hardware CA HSM are performed during the key ceremony in front of witnesses including a bailiff in secured premises. This activation data is stored on smartcards and given to key custodians. Each key custodian take all necessary precautions to prevent the loss, theft, unauthorized disclosure or unauthorized use of the smartcards and the activation data stored within.

6.4.2 Activation data protection

The activation data are stored within nominative and personal smartcards. Each card is under the responsibility of the person it belongs to and is protected by a PIN known only by the card holder. Smartcard are stored in individual safes when not in use. Each card holder is responsible for the safeguard of the card containing the activation data and sign an agreement acknowledging his responsibilities.

6.4.3 Other aspects of activation data

Activation Data Transmission
If a smartcard 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 Hardware 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 Hardware CA has appropriate platform-oriented controls in place (such as antivirus, antimalware, ...) to prevent unauthorized or illegitimate software from running within its systems.

Each Hardware 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 information is stored in such a way it can only be accessed by authorized users.

Access control:

Profiles and access rights to the PKI equipment 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, 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.

Access control procedures ensure that system administrators in Universign's network do not have access to certificate issuance systems.

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 life clycle tracking procedures to ensure the traceability and 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.

Capacity demands are monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.

Component integrity:

The components of the local network are kept in a physically secure environment. Periodic compliance checks 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 set up to ensure the authentication of the origin, 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 records and allow rapid reaction against any unauthorized or abnormal attempt to access resources (physical and/or logical).

Awareness:

Awareness procedures for personnel have been set up.

6.5.2 Computer security rating

Not applicable.

6.6 Lifecycle technical controls

6.6.1 System development controls

All software componants of the PKI developped by Universign are developped in conditions and following a process that ensures their security. Universign uses quality process during design and developement 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 Lifecycle security controls

Not applicable.

6.7 Network security controls

The Hardware CAs are implemented on a network protected with firewalls that segment the systems into networks according to their sensitivity. These firewalls are configured to accept only connections which are strictly necessary. The network is redundant to ensure the availability of the services. Moreover, the criticals components are placed in the securiest areas.

The network communications transfering 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.

Hardware 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.

Hardware CA maintains access control procedures to separate administrative and operationnal practices. All functions (publication, certificate generation, revokation) need an authentication to be executed. Hardware CA maintains an access control policy to limit functions access to authorized people in trusted roles only.

6.8 Timestamping

All the servers of the Universign Hardware CA are synchronized with the same time source (UTC). The synchronization of all the servers is regularly checked by Universign, at least daily.

7 Certificate, CRL and OCSP profiles

7.1 Certificate profiles

All certificats issued by Universign comply with X.509, [ETSI 319 412-2] and [ETSI 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	V3
Serial Number	defined by the tool
Signature	RSA/SHA-256
Issuer DN	C=FR, O=Cryptolog International, OU=0002 43912916400026, CN=`Universign Primary CA hardware`
Validity	10 years
Subject DN	C=FR, O=Cryptolog International, OU=0002 43912916400026, CN=`Universign CA hardware`
Public Key	RSA 2048 bits

Certificate extension

Field	OID	Critical	Value
Authority Key Identifier	2.5.29.35	No	
KeyIdentifier			RFC 5280 - Method 0
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
Basic Constraint	2.5.29.19	Yes	
CA			True
Maximum Path Length			0 [12]
CRL Distribution Points	2.5.29.31	No	
fullName			http://crl.universign.eu/universign_primary_ca_hardware.crl [13]
reasons			Absent
cRLIssuer			Absent
Certificate Policies	2.5.29.32	No	
policyIdentifier			2.5.29.32.0
policyQualifierId			1.3.6.1.5.5.7.2.1
qualifier			http://docs.universign.eu/

[12] The current CP/CPS limits the path of length to 0.

[13] This URL is given as an example and may be changed. Users shall only trust the URL within the certificate.

7.1.2 Certificate of the Subscriber

Base fields

Certificate for physical person

Field	Value
Version	v3
Serial Number	defined by the tool
Signature	RSA/SHA-256
Issuer DN	C=FR O=Cryptolog International OU=0002 43912916400026 CN=`Universign CA hardware`
Validity	5 years
Subject DN	C=Country Code of the certificate holder O= Legal name of the attached organization, if applicable OI= Unique identification number of the organization, if applicable givenName= Last name of the Subject surnmame= First name of the Subject CN= Last name and first name used by the Subject SERIALNUMBER= Defined by the tool.
Public Key	RSA 2048 bits

Certificate for entity or organization

Field	Value
Version	v3
Serial Number	defined by the tool
Signature	RSA/SHA-256
Issuer DN	C=FR O=Cryptolog International OU=0002 43912916400026 CN=`Universign CA hardware`
Validity	5 years
Subject DN	C=Country of the entity or organization O= Legal name of the organization OI= Unique identification number of the organization CN= Free field referring to the organization
Public Key	RSA 2048 bits

Certificate extension

Qualified certificate for Physical Person

Field	OID	Critical	Value
Authority Key Identifier	2.5.29.35	No	
KeyIdentifier			RFC 5280 - Method 0
Subject Key Identifier	2.5.29.14	No	
KeyIdentifier			RFC 5280 - Method 1
Key Usage	2.5.29.15	Yes	
digitalSignature			True
nonRepudiation			True
keyEncipherment			False
dataEncipherment			False
keyAgreement			False
keyCertSign			False
cRLSign			False
encipherOnly			False
decipherOnly			False
Basic Constraint	2.5.29.19	Yes	
CA			False
CRL Distribution Points	2.5.29.31	No	
fullName			http://crl.universign.eu/universign_subordinate_ca_hardware.crl [14]
reasons			Absent
cRLIssuer			Absent
Certificate Policies	2.5.29.32	No	
policyIdentifier			1.3.6.1.4.1.15819.5.1.3.1
policyQualifierId			0.4.0.194112.1.0
qualifier			http://docs.universign.eu/
Qualified Certificate Statements	1.3.6.1.5.5.7.1.3	No	
Qualified Certificate [15]	0.4.0.1862.1.1		
PDS URL [16]	0.4.0.1862.1.5		https://docs.universign.eu/sub_pds.pdf
Certificate's type OID [17]	0.4.0.1862.1.6		0.4.0.1862.1.6.1[18]
Authority Info Access	1.3.6.1.5.5.7.1.1	No	
fullName			http://scah.ocsp.universign.eu/

[14] URLs for information purposes only. Users shall only trust the URL within the certificates.
[15] Corresponding to esi4-qcStatement-1
[16] Corresponding to esi4-qcStatement-5
[17] Corresponding to esi4-qcStatement-6
[18] Corresponding to id-etsi-qct-esign

Not qualified certificate for Physical Person

Field	OID	Critical	Value
Authority Key Identifier	2.5.29.35	No	
KeyIdentifier			RFC 5280 - Method 0
Subject Key Identifier	2.5.29.14	No	
KeyIdentifier			RFC 5280 - Method 1
Key Usage	2.5.29.15	Yes	
digitalSignature			True
nonRepudiation			True
keyEncipherment			False
dataEncipherment			False
keyAgreement			False
keyCertSign			False
cRLSign			False
encipherOnly			False
decipherOnly			False
Basic Constraint	2.5.29.19	Yes	
CA			False
CRL Distribution Points	2.5.29.31	No	
fullName			http://crl.universign.eu/universign_subordinate_ca_hardware.crl [19]
reasons			Absent
cRLIssuer			Absent
Certificate Policies	2.5.29.32	No	
policyIdentifier			1.3.6.1.4.1.15819.5.1.3.3
policyQualifierId			0.4.0.2042.1.3
qualifier			http://docs.universign.eu/
Authority Info Access	1.3.6.1.5.5.7.1.1	No	
fullName			http://scah.ocsp.universign.eu/

[19] URLs for information purposes only. Users shall only trust the URL within the certificates.

Qualified certificate for entity or organization

Field	OID	Critical	Value
Authority Key Identifier	2.5.29.35	No	
KeyIdentifier			RFC 5280 - Method 0
Subject Key Identifier	2.5.29.14	No	
KeyIdentifier			RFC 5280 - Method 1
Key Usage	2.5.29.15	Yes	
digitalSignature			True
nonRepudiation			True
keyEncipherment			False
dataEncipherment			False
keyAgreement			False
keyCertSign			False
cRLSign			False
encipherOnly			False
decipherOnly			False
Basic Constraint	2.5.29.19	Yes	
CA			False
CRL Distribution Points	2.5.29.31	No	
fullName			http://crl.universign.eu/universign_subordinate_ca_hardware.crl [20]
reasons			Absent
cRLIssuer			Absent
Certificate Policies	2.5.29.32	No	
policyIdentifier			1.3.6.1.4.1.15819.5.1.3.5
policyQualifierId			0.4.0.194112.1.1
qualifier			http://docs.universign.eu/
Qualified Certificate Statements	1.3.6.1.5.5.7.1.3	No	
Qualified Certificate [21]	0.4.0.1862.1.1		
PDS URL [22]	0.4.0.1862.1.5		https://docs.universign.eu/sub_pds.pdf
Certificate's type OID [23]	0.4.0.1862.1.6		0.4.0.1862.1.6.2[24]
Authority Info Access	1.3.6.1.5.5.7.1.1	No	
fullName			http://scah.ocsp.universign.eu/

[20] URLs for information purposes only. Users shall only trust the URL within the certificates.
[21] Corresponding to esi4-qcStatement-1
[22] Corresponding to esi4-qcStatement-5
[23] Corresponding to esi4-qcStatement-6
[24] Corresponding to id-etsi-qct-eseal

Not qualified certificate for entity or organization

Field	OID	Critical	Value
Authority Key Identifier	2.5.29.35	No	
KeyIdentifier			RFC 5280 - Method 0
Subject Key Identifier	2.5.29.14	No	
KeyIdentifier			RFC 5280 - Method 1
Key Usage	2.5.29.15	Yes	
digitalSignature			True
nonRepudiation			True
keyEncipherment			False
dataEncipherment			False
keyAgreement			False
keyCertSign			False
cRLSign			False
encipherOnly			False
decipherOnly			False
Basic Constraint	2.5.29.19	Yes	
CA			False
CRL Distribution Points	2.5.29.31	No	
fullName			http://crl.universign.eu/universign_subordinate_ca_hardware.crl [25]
reasons			Absent
cRLIssuer			Absent
Certificate Policies	2.5.29.32	No	
policyIdentifier			1.3.6.1.4.1.15819.5.1.3.4
policyQualifierId			0.4.0.2042.1.3
qualifier			http://docs.universign.eu/
Authority Info Access	1.3.6.1.5.5.7.1.1	No	
fullName			http://scah.ocsp.universign.eu/

[25] URLs for information purposes only. Users shall only trust the URL within the certificates.

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 CA hardware`
Next Update	This Update + 7 day

CRL Extension

Field	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

Universign may propose status of issued certificates via OCSP (Online Certificate Status Protocol). OCSP is a way to obtain information about the revocation status of a particular certificate without downloading the CRL. Universign OCSP is supporting RFC 5019 standard.

OCSP Extensions The current freshness of each OCSP response is established by the use of a validity date. Therefore, no nonce are used by Universign OCSPs to establish this freshness. Thus clients should not expect a nonce in the response to a request that contains a nonce.

8 Compliance audit and other assessments

8.1 Frequency or circumstances of assessment

An audit ensuring compliance to this CP shall be performed at the start of the PKI and after each major modification.

Two kinds of compliance audit are made:

- an internal audit;
- a [ETSI 319 411-1] conformance audit performed by an accredited organization at least every 2 years.
- a [ETSI 319 411-2] conformance audit performed by an accredited organization at least every 2 years.

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. Hardware CAs commit 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

For internal audit, 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 targeted Hardware CA. For certification audit, the assessor must be independant andshall not have a conflict of interest that hinders their ability to perform Hardware CA audit.

8.4 Topics covered by assessment

The assessor carries out compliance audits for the specified component, covering either in full or in part the implementation of:

- the CP/CPS;
- the components of the PKI, including the potential sub-contractors.

Prior to each audit, the assessor will provide the Hardware CA Approval Board with a list of components and procedures he or she wishes 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 Approval Board of the Hardware CA the result which can be “success”, “failure” or “to be confirmed”.

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

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

In case of success, the Hardware CA confirms the compliance with the requirements of the CP/CPS.

8.6 Communication of results

The audit results of the Hardware CA are made available to the qualification organism in charge of the certification of the Hardware CA .

9 Other business and legal matters

9.1 Fees

9.1.1 Certificate issuance or renewal fees

A Hardware CA may charge Subscribers for certificate issuance services.

9.1.2 Certificate access fees

Hardware CA repositories and issued certificated are accessible free of charge.

9.1.3 Revocation or status information access fees

Hardware CA LCRs publication services and revocation services are accessible free of charge. However, a Hardware CA may charge for extra advanced LCR and revocation services, running in parallel of the free ones.

9.1.4 Fees for other services

A Hardware CA offers free consultation access to this CP/CPS. Any other use made of this CP/CPS, including but not limited to reproduction, redistribution, modification or creation of derivative contents, is subject to approval from Universign and may be subject to a license agreement.

9.1.5 Refund policy

Universign does not apply a refund policy, in the limit of the applicable laws.

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, particularly Subscribers, 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/CPS.

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 Hardware CAs,
- activation data linked to the private keys of the Hardware CAs,
- event journals,
- the registration files (accepted and refused ones),

- audit reports,
- recovery, continuity and end of activity plans,
- revocation cause of the certificates.

Other datas can be classified as confidential, particularly if they are shown to be sensible after a risk analysis (See Section 5.2.5).

9.3.2 Information not within the scope of confidential information

Universign repository and its content (Hardware CA certificates, CRLs, certificate information status,...) is not considered confidential.

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

Data within registration file that are not published in certificates or CRLs are considered as confidential data.

9.4.3 Information not deemed private

No specific commitments.

9.4.4 Responsibility to protect private information

Universign is responsible for the process of the personal data in the meaning of the article 3 of the law 78-17 of the January 6, 1978 modified in 2004.

9.4.5 Notice and consent to use private information

Unless cases stated within this CP/CPS, within the Subscriber Agreement or within aggreement between the Hardware CA and the Subscriber, Universign shall not use the private data without authorisation, in the limits of applicable laws.

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 developed by Universign to operate 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 punishable by the "Intellectual Property Code", unless Universign has previously given its written consent for such use.

Intellectual Property of Certificate and Revocation Information Universign holds the intellectual property rights on the certificates and revocation information issued by Universign. Universign allows the copy and distribution of issued certificates if and only if:

- there is no commercial use of the issued certificate;
- certificates are not modified in any way;
- the certificate is used in accordance with the Relying Parties Agreement.

Universign allows the use of the information relative to revocation status in accordance with the Relying Parties Agreement.

Intellectual Property of this CP/CPS Intellectual Property of this CP/CPS is owned by Universign.

Intellectual Property of the name

Any Subscribers shall retain the intellectual property, if applicable, of trademarks and tradenames present in the registration or in the DN field of the issued certificate.

Intellectual Property of the keys Hardware CAs keys belong to Universign. Subscribers keys are the property of each Subscriber. Activation data of the Hardware CAs is the property of Universign.

9.6 Representations and warranties

The components of the PKI must ensure that they:

- 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/CPS and its subsequent documents;
- submit to the compliance audit carried out by the assessment team appointed by the Hardware CA;
- document their internal processes;
- implement the measures (technical and human) necessary to meet their 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/CPS;
- compliance of the issued certificate with this CP/CPS;
- abidance to the security principles for all the components of the PKI and their subsequent controls.

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

- the informations contained if the certificate does not match the registration informations;
- the Hardware 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 Subscriber must:

- communicate correct and up to date information when requesting a Subscriber certicate;
- protect the private key under his responsibility;
- abide by the conditions of use of the private key according to what is established in this CP/CPS;
- inform the Hardware CA of any modification regarding the information contained in the Subscriber certificate;
- immediatly performs a revocation request of a Subscriber certificate in case of suspected compromise of the corresponding private key.

The Subscriber is registrated with the Hardware CA according to the process defined in this CP/CPS.

9.6.4 Relying party representations and warranties

Relying Parties using certificates from the Hardware CA must:

- verify and adhere to by the usage for which the certificate has been issued;
- verify the revocation status of the certificate;
- verify and adhere by the obligations defined in this CP and in the Relying Parties Agreement.

9.6.5 Representations and warranties of other participants

Certification Representative The Certification Representative is responsable for:

- identification of individual and validation of the link to the entity or organisation;
- conformity of the registration process with this CP/CPS.

9.7 Disclaimers of warranties

Disclaimers of waranties are described in the Subscriber Agreement and the Relying Parties Agreement, and are applicable to the entente permitted by effective laws.

9.8 Limitations of liability

Universign cannot be held liable for non-authorized or non-compliant by the current CP/CPS for the usage of the certificates, the associated private keys, the revocation status information or 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, under no circumstances 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's responsibility will be limited to the amount paid by the Subscriber to Universign the last six months, with respect to the governing law. Unless otherwise legally enacted, any lawsuit from the Subscriber regarding these CP will take place no longer than six months after the fact originating the legal action.

9.9 Indemnities

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

9.10 Term and termination

9.10.1 Term

This CP/CPS is effective as soon as it is published on Universign repository and the request for comment period has expired. This CP/CPS remains in effect until the expiration of the last certificate issued under it.

9.10.2 Termination

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

9.10.3 Effect of termination and survival

At termination of this CP/CPS, PKI participant are still under the conditions of this CP/CPS for allcertificates issued during the validity period, until the expiration of the last certificate.

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/CPS 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, approval, maintenance and modifications of the current CP/CPS.

When a new version of the CP/CPS is approved by the Universign Approval Board, it will be published on the Universign web site and will replace the terms of the previous version after the request for comments period.

9.12.2 Notification mechanism and period

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

When a new version of the CP/CPS 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 the Universign web site.

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

Unless otherwise stated, the new version of the CP/CPS 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 AFOREMENTIONNED 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].

9.16 Miscellaneous provisions

9.16.1 Entire agreement

Not applicable.

9.16.2 Assignment

Not applicable.

9.16.3 Severability

Dans le cas où une disposition de la CP/CPS s'avérerait être invalide, illégale ou non exécutoire de l'avis d'un tribunal de la juridiction compétent, la validité, la légalité et le caractère exécutoire des autres clauses ne seront en aucun cas affectées ou réduites.

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 activites 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.

References

[**RFC 3647**]
Network Working Group - Request for Comments: 3647 - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework - (2003-11)

[**RFC 5280**]
Network Working Group - Request for Comments: 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (2008-05)

[**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.