Universign Primary CAs

Certification Policy
Certification Practice Statement

OID: 1.3.6.1.4.1.15819.5.1.2.1
1.3.6.1.4.1.15819.5.1.2.2

VERSION : 2.1	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.
Each Primary CA aims to be certified in accordance with [**ETSI 319 411-1**] level NCP+.

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 Primary CAs and the certification practice statement of the Primary CAs. This document defines Universign commitments, in terms of security, procedures and requirements regarding the issuance of certificates by the Universign Primary CAs.

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

- Primary CAs;
- Subordinate CAs, linked to at least one Primary CA;
- End-users.

A Primary CA only delivers certificates to Subordinate CAs that meet the requirements described in Appendix A of this CP/CPS. Subordinate CAs only deliver certificates to end-users, which can be physical persons or organisations.

The current CP/CPS document does not allow a Subordinate CA to deliver certificates to other Primary CAs. Further versions of this CP/CPS may consider this use case. The current CP/CPS only considers two classes of certificates, according to the requirements of Appendix A.

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

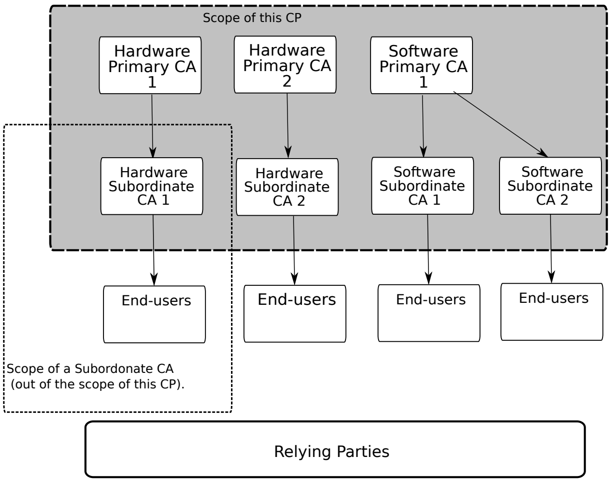
Scope of this CP
Hardware Primary CA 1
Hardware Primary CA 2
Software Primary CA 1
Hardware Subordinate CA 1
Hardware Subordinate CA 2
Software Subordinate CA 1
Software Subordinate CA 2
End-users
End-users
End-users
End-users
Scope of a Subordonate CA (out of the scope of this CP).
Relying Parties

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

Scope of this CP/CPS The scope of this CP/CPS focuses on Primary CAs and delivering certificates to Subordinate CAs. Each Subordinate CA shall provide its own CP and its own CPS in conformance with the requirements defined in Appendix A of this CP/CPS. Certificate delivery to end-users is out of the scope of this CP/CPS and shall be described in Subordinate CAs's CP and CPS.

This CP/CPS defines the following PKI participants:

- Primary CAs, delivering certificates to Subordinate CAs that meet the requirements defined in Appendix A of this CP/CPS;
- Subordinate CAs, which are certificate holders of the Primary CAs;
- Users, whose operations depend on the UTN.

1.2 Document name and identification

This document is the Certification Policy of the Universign Primary CAs. It also includes 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 Primary CA:

- 1.3.6.1.4.1.15819.5.1.2.1 for Hardware Primary CA;
- 1.3.6.1.4.1.15819.5.1.2.2 for Software Primary CA.

1.3 PKI participants

1.3.1 Certification Authorities

A certification authority is an umbrella term designating an authority that can issue certificates to certificate holders. Within the Universign Trusted Network, two kind of entities correspond to that generic description:

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

The scope of this CP/CPS focuses on the Primary CAs and the issuance of certificates to the Subordinate CAs (see Section 1.1). Therefore, in the scope of this CP/CPS, the Subordinate CAs are the certificate holders. Consequently, in the scope of this PC, the term CA only refers to the Primary CAs.

Primary CA Management The CA is managed by the Universign Approval Board. Universign executive management sits on 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 Primary CA documentation corpus.
- approving the CP/CPS;
- defining the update process for the CP/CPS, with the responsibility of maintaining 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 Subordinate CAs and Relying Parties.

1.3.2 Registration Authorities

A Registration Authority (RA) is an entity that delivers services for the identification and authentication of the physical person that will hold the certificate.

In the scope of this CP/CPS, each Primary CA acts as an RA. This CP/CPS defines the responsibilities of Universign acting as an RA.

1.3.3 Certificate Owners

A certificate owner is generic term that can cover the following:

- The Subject: an individual, entity or organisation named in the `subject` field of the certificate;
- The Subscriber: an individual, entity or organisation that enters into a contract with the certificate issuer;
- The administrative contact; an individual that has the responsability for the issued certificate and its lifecycle (certificate request, revocation,...).

Depending on the architecture, these persons and/or entities may be the same entity or person or may be separate entities or persons.

In the scope of this CP/CPS, we define the following:

- The Subject must be a Certification Authority, called *Subordinate CA* in this document. This Subordinate CA is defined in the `subject` field of the certificate issued.
- The Subscriber is the entity owning the Subordinate CA. This entity can be:
  - Universign or one of its affiliates;
  - A third party organisation contracting with Universign or one of its affiliates.
- The entity owning the Subordinate CA shall name an administrative contact. This person is called *Primary Contact* in the present document.

To be part of the UTN, the Subordinate CAs shall comply with the registration process defined in this CP/CPS (see Section 4.1). In particular, the Subordinate CAs shall comply with the requirements defined in Appendix A.

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 Primary CA, particularly the association between the Subordinate CA and the public key. A Relying Party is responsible for deciding how to check the validity of a Subordinate CA Certificate, at least by checking the appropriate certificate status information. A Relying Party may use information in the Certificate (such as Certificate Policy identifiers) to determine the suitability of the Certificate for a particular use.

1.3.5 Other Participants

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

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

Universign maintains a list of the Primary Trusted Parties and notifies them when major events occur during the Primary CA lifecycle (see Appendix B).

1.4 Certificate Usage

1.4.1 Appropriate certificate uses

The Subordinate CAs keys can be used for signing:

- X.509 v3 Subordinate CA certificates
- Its CRLs and/or its OCSP responses
- Technical certificates of the components that make up its infrastructure.

1.4.2 Prohibited certificate uses

Any usage other than those defined in the previous paragraph is prohibited by this CP. In particular, the present CP/CPS does not allow a Subordinate CA to issue a certificate to a Certification Authority. 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
Primary 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

The Universign Approval Board determines the suitability and applicability of this CP/CPS.

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 Primary 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 Primary CA published information is the following:

- this CP/CPS[2];
- the applicable CRLs, in accordance with the Requirements of this CP/CPS;
- the active certificates of the Universign Primary CAs and their hash.
- the PKI Disclosure Agreement;
- the Relying Parties Agreement;

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 Primary 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).

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

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

For a Subordinate CA, requirements relative to time and frequency of publication of information are defined in Appendix A.

[2] 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 conform to the specifications of the X.500 standard.

The Primary CA and Subordinate CA are identified by an explicit name (called "DN" hereafter) of type X.501. This type of DN is defined in chapter 7. All certificates issued by a Universign Primary CA shall contain the following fields:

Field	**Mandatory**	**Semantics**	**Verified by RA**	**Document used for verification**
C	Yes	Country	Yes	Valid and legal organization identification document
ST	No	State of the entity owning the Subordinate CA	Yes	Valid and legal organization identification document
L	No	City of the entity owning the Subordinate CA	Yes	Valid and legal organization identification document
O	Yes	legal name of the organisation owning the Subordinate CA	Yes	Valid and legal organization identification document
OU	Yes	Unique identification number of the organization owning the Subordinate CA[3] structured in accordance with ISO 6523	Yes	Valid and legal organization identification document
CN	Yes	Free field referring to the organization owning the Subordinate CA	Yes [4]	

[3] For a French company, 0002 followed by one space and the SIREN or SIRET number

[4] It will only be checked that the name is meaningful (see Sect. 3.1.2)

The details of the process of identification of a Subordinate CA by the Universign Primary CA are described in chapter 3.2.2 and chapter 3.2.3.

3.1.2 Need for names to be meaningful

Universign Primary CAs delivers certificates only if they include meaningful DN in the following sense: Certificates shall contain names with commonly understood semantics permitting the determination of the identity of the individual or organization that is the Subject of the Certificate. The Universign Approval Board has the authority to decide if a name is meaningful or not.

3.1.3 Anonymity or pseudonymity of subscribers

These practices are not allowed.

3.1.4 Rules for interpreting various name forms

No stipulation.

3.1.5 Uniqueness of names

The names of Subordinate CAs shall be unique for a given Primary CA. This verification is performed by the RA during the registration[5]. It is possible for a Subordinate CA to have two or more certificates with the same Subject Distinguished Name (DN) within UTN.

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.

[5] A Primary CA issues certificates only to Subordinate CAs, so since the number of certificates is limited, a manual verification is performed and is sufficient.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

At the time of the certificate application, the Primary 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 to be done by using the Subordinate CA private key to sign a PKCS#10 certificate request (or equivalent cryptographic mechanism accepted by Universign) and providing that request to the Primary CA.

3.2.2 Authentication of organization identity

The validation of identity Subordinate CA entity is done through the validation of the identity of its Primary Contact. This practice is justified by the fact that each Subordinate CA has only one Primary Contact at any given time.

3.2.3 Authentication of individual identity

The individual identity of the representative of the Subordinate CA Entity is checked by the RA against a physical person during a face to face meeting. Universign only requieres the elements needed to issue the certificate. Evidence of the individual is verified by RA using:

- a form signed by the authority of the organization, explicitly authorizing the Primary Contact to act on behalf of the organization. The name of the Primary Contact shall be explicitly mentioned and the form shall be signed by the Primary Contact. Date of signature shall not be more than three months prior to the date of the beginning of the subscription process.
- a legal national document proving the existence of the organisation, valid at the certification request (typically a Kbis for a French company). This document shall have a unique legal identification number of the company (for example SIRET number for a French company).
- official ID Document including a recent picture, the place and date of birth of the subject;
- the postal address and email so that the Primary Contact can be reached by the Primary CA.

A copy of these elements is part of the registration file of the Subordinate CA and is kept by the Primary CA Universign in a safe place.

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 Primary CA validates the authority of a Subordinate CA representative with a mandate signed by the legal representative of the organization, as described in Section 3.2.3.

3.2.6 Criteria for interoperation

A Subordinate CA which is certified by the Primary CA Universign adheres to the requirements defined in Appendix A.

3.3 Identification and authentication for re-key requests

The Primary 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

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

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

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

If the above conditions are met, the Primary CA signs the revocation request and transmits it to the Universign teams who perform the technical steps of the revocation.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate application

4.1.1 Who can submit a certificate application

For a given Subordinate CA, the Primary Contact can submit certificate applications to a Primary CA.

4.1.2 Enrollment process and responsibilities

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

- if the Subordinate CA is not owned by Universign or subsidiaries, the Subordinate CA must enter in a formal agreement with the Primary CA;
- the Primary Contact completes a Certificate Application Form filled with correct information. The Primary Contact shall provide all elements of the registration record, in particular evidence that the Subordinate CA satisfies the requirements of Appendix A;
- the Subordinate CA shall generate its own keypair;
- the Primary Contact shall provide the public key of the Subordinate CA to the Primary CA;
- the Primary Contact shall provide evidence that the Subordinate CA owns the private key associated with the public key.

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

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Universign Primary CA handles the RA function itself. Some parts of the registration process may be handled by third parties under contract with Universign. The

RA validates Certification Requests of the Subordinate CAs. The RA performs identification and validation of all required information provided by Subordinate CAs in conformance with section 3.2.

4.2.2 Approval or rejection of certificate applications

The process is the following:

- the Primary CA Universign, as an RA, checks the certificate request form is complete and accurate;
- the Primary CA Universign successfully authenticates the requestor and the information provided, in line with section 3.2. In particular, the Primary CA verifies the evidence of compliance with the appendix A;
- the Approval Board finally decides whether it accepts the request or not [6].

If the request is rejected, the Primary Contact is immediately informed of the reason. The Primary CA may, at any step, ask the Subordinate CA to provide additional evidences or to justify its compliance with this CP/CPS.

4.2.3 Time to process certificate applications

A Primary CA begins processing certificate applications within a reasonable time of receipt. Unless stipulated in the contract between a Primary CA and a Subordinate CA, there is no minimal delay. A certificate application remains active until rejected.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

A Primary 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 premisesby two members of staff in a Trusted Role.

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

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

[6] The Approval Board can refuse any Subordinate CA for non-technical reason.

4.3.2 Notification to subscriber by the CA of issuance of certificate

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

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

Subordinate CA certificate acceptance must be done in a formal way by a document sent to the Primary CA. Failure of the Subordinate CA to send the formal acceptance within a reasonable time after several reminders will result in revocation of the certificate by the Primary CA.

4.4.2 Publication of the certificate by the CA

A Primary CA does not publish the issued certificates without explicit authorization of the Subordinate CA.

4.4.3 Notification of certificate issuance by the CA to other entities

Upon certificate acceptance, the Primary Trusted Parties (see Appendix B) are notified.

4.5 Key pair and certificate usage

Subordinate CA:

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 Primary CA and the Subordinate CA, if applicable;
- the `KeyUsage` extension defined in certificate or any extension within the certificate that constrains the key usage.

In line with the requirements of Appendix A, a Subordinate CA shall

- protect its private keys;

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

Relying Parties:

Relying Parties must accept the Relying Parties Agreement before any use of certificate issued by a Primary 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 Primary 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 Primary 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 Primary CA the are the following:

- the Primary CA receives a motivated revocation request from the Subordinate CA;

- a Subordinate CA does not respect or has not respected its obligations regarding the Primary CA, in particular the requirements defined in Appendix A;
- the information regarding a Subordinate CA included in the certificate are no longer accurate;
- Primary CA or Subordinate CA strongly suspects the loss or theft of a private key, or that it has been compromised;
- error in the registration procedure;
- end of contract between a Primary CA and a Subordinate CA;
- if applicable, no payment for the certificate issuance;
- definitive end of activity of a Primary CA;
- a Subordinate CA 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

The persons who can request revocation of a Subordinate CA certificate are:

- the Universign Approval Board;
- the Primary Contact of the Subordinate CA.
- a legal representative of the entity operating the Subordinate CA.

4.9.3 Procedure for revocation request

The Primary Contact (or the Approval Board) transmits a revocation request which contains at least the following information:

- Subordinate CA identification (see Sect. 3.1.1);
- Serial number of the Subordinate CA certificate to be revoked;
- Subordinate CA administrative contact full name;
- (possibly) the reason for revocation. This reason is for information purposes only and is not listed in the CRL.

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

The Universign Primary CA informs the revoked certificate Primary Contact 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, 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. For that, Relying Parties can consult the most recent CRL from the Primary CA that has issued the certificate. This CRL is publicly available, as defined in Section 4.10.1.

4.9.7 CRL issuance frequency

CRLs are issued at least every 60 minutes.

4.9.8 Maximum latency for CRLs

CRLs are published in a reasonable delay after their generation. In general, publication is done automatically at most 30 minutes after the CRLs generation.

4.9.9 Availability of an online revocation/status checking system

Not applicable.

4.9.10 Online revocation checking requirements

Not applicable.

4.9.11 Other forms of information about revocations available

Not applicable.

4.9.12 Special requirements regarding key compromise

Universign will directly and immediately notify all the Primary Trusted Parties (see Section B) as soon as the compromise of the key is discovered.

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 are posted on a freely accessible publication site

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

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

4.10.2 Service availability

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

4.10.3 Optional features

Not applicable.

4.11 End of subscription between a Primary CA and a Subordinate CA

The end of subscription between a Primary CA and a Subordinate CA falls under the scope of the contract between a Primary CA and a Subordinate CA, 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 Primary 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 Primary 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 Primary CA facilities is strictly restricted to authorized personnel listed on an access list. A logbook is updated each time maintenance is operated on the Primary 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.

Primary CAs are operated in the most secure tier. Access to this tier can only be carried out by authorized personal under dual control.

5.1.3 Power and air conditioning

Emergency controls are operated so that a disruption of power supply, or an air conditioning failure do not jeopardize Universign's commitments in terms of availability.

5.1.4 Water exposure

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

5.1.5 Fire prevention and protection

Secured areas benefit from appropriate prevention and protection against fire. 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 Primary CA in secured locked premises and stored in a safe and the means of opening this safe are known only by the Primary CA Chief Officer and authorized personnel.

Primary CAs ensures 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. In particular, the following destruction processes apply:

- Paper/ CD / smartcards: these media are shredded before waste disposal;
- HSMs: HSMs are zeroized, and, if needed, made unusable following the recommendations of the manufacturer;
- Storage Media: these are made unreadable using an appropriate method before waste disposal.

5.1.8 Off-site backup

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

Universign ensures that backups are performed by Trusted Role.

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

Universign ensures that back-up are regularly tested to ensure that they meet the requirements of business continuity plans.

5.2 Procedural controls

5.2.1 Trusted roles

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

The following Trusted Roles are defined:

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

Primary CA personal in Trusted Role (and more generally, all Primary CA personal) shall be free of conflicting interests that might prejudice the impartiality of the operations. Personnel in trusted roles are appointed with written notifications by Primary CA senior management. Universign regularly ensures that all the trusted roles are filled in order to guarantee the activity continuity.

5.2.2 Number of persons required per task

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

5.2.3 Identification and authentication for each role

Identification and authentication controls are defined in order to support the implementation of the access control policy and the accountability of operations.

The access control policy limits access to authorized personnel on a need to know basis.

5.2.4 Roles requiring separation of duties

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

Each Primary 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 Primary CAs. This risk analysis is periodically reviewed and each time a structural change occurs on a Primary CA. Moreover, the risk analysis methodology allows Universign to ensure that its inventory is kept up to date.

5.3 Personnel controls

The Universign Primary CA employs a sufficient number of personnel which possess the expert knowledge, experience and qualifications necessary for the services offered and as appropriate to the job function.

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/her responsibility through his/her job description and/or procedures related to system security and personnel control. Trusted Roles are appointed by Universign management.

5.3.2 Background check procedures

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

- the personnel is free from conflict interests;

- the personnel does not have a conviction for a serious crime or other offence.

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

5.3.3 Training requirements

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 Primary CA . Subcontractors can have access to Universign secure premises only under the responsability and control of persons under Trusted Role.

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 Primary CAs key life cycle events;
- all life cycle events of certificates issued by Primary 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 Primary 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 processed on daily basis and 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 backed up 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 is made.

5.4.8 Vulnerability assessments

The Universign Primary CA cannot be accessed through a network and implements the following measures:

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

These measures allow the CA to detect:

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

5.5 Archival of records

5.5.1 Types of records archived

The data archived are the following:

- the registration files of the Primary Contacts;
  - evidence of acceptance of the Subscriber Agreement by the Subordinate CAs (see Section 4.1.2);
  - the Subordinate CAs registration request forms (see Section 4.1.2);
  - copies of elements used to verify the identity of the Primary Contact (see Section 3.2.3);

  - copies of elements used to verify the identity of the link between the Primary Contact and the Subordinate CA (see Section 3.2.2);

- the audit logs. In particular:
  - significant Primary CA environmental change events and their time;
  - key management and certificate management events and their time.

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

5.5.2 Retention period for archive

Subordinate CA registration forms:
The Subordinate CA registration forms are kept for the whole life of the Primary 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 Primary CA signing key, the Primary CA shall generate a new certificate-signing key pair and shall apply all necessary actions to avoid disruption to the operations of any entity that may rely on the Primary CA key. The new Primary 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 set up processes and technical means to report and handle incidents (awareness, personnel training, audit log analysis, ...). In this way, Primary CAs minimize damages in case of incident.

The Primary CA has set up an incident response plan to respond to the 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 Primary CA private key for instance, is immediately reported to the Primary CA Approval Board, which, if necessary, may then decide to terminate the Primary CA.

Universign possesses a list of contacts to be notified in the cases described above (see Appendix B). Universign will directly and immediately notify each contact in the list.

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

An Activity Continuity Plan has been set up in order to ensure the business continuity of all PKI components.

5.7.3 Entity private key compromise procedures

This point is covered by the business continuity and business recovery plan. The compromising of a key of the Primary CA will lead to the immediate revocation of all issued certificates. In such a case, the various participants will be notified that the CRL may not necessarily be fully trusted. Similar procedures are applied if any of the algorithms, or associated parameters, used by the Primary CA or its Subordinate CAs become insufficient for its remaining intended usage.

5.7.4 Business continuity capabilities after a disaster

The ability to continue activity after a disaster is described in Universign Disaster Recovery Plan. After a disaster the Primary CA performs this plan to reactivate the stopped services. In particular, each critical service of a Primary CA has a backup service. Moreover, Universign have spare hardware to supply any hardware failure. In cas of major disaster, Universign has a recovery plan allowing the setup of a new Primary 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 Primary 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, Primary Trusted Parties (see Appendix B) and other entities with which the Primary CA has agreements (in particular to forbid the process of all new registration requests);

2. potential revocation of all issued certificate which are still valid;

3. fate of the Primary CA private key, that must be destroyed or put beyond use;

4. necessary undertakings to transfer obligations for maintaining registration information, revocation status information and event log archives for their respective period of time as indicated to the Subordinate CAs and relying party;

5. publication of the corresponding information for the relying parties.

This plan is checked and updated on a regularly basis.

6 Technical security controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

Primary CA Keys:
Primary 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.

Subordinate CA Keys:
Requirements for Subordinate CAs are defined in Appendix A.

6.1.2 Private key delivery to Subordinate CA

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

6.1.3 Public key delivery to Primary CA

The Subordinate CA public key is delivered on site to the Primary CA by the Primary Contact during a face-to-face meeting.

6.1.4 CA public key delivery to relying parties

Universign Primary CAs root certificates together with their hash are published on the site: `http://docs.universign.eu`.

The certificates must contain all the informations described in chapter 7 of this CP/CPS.

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

6.1.5 Key sizes

The keys used by the Universign Primary CA have the following characteristics (or stronger or equal cryptographic characteristics):

Certificate	**Key Size**	**Format**
Primary CA	2048	RSA

The keys of the Subordinate CAs and the customer of the subscribers must meet the requirements of Appendix A.

6.1.6 Public key parameters generation and quality checking

The key generation material and algorithms (see Sect. 6.2.11) use parameters that meet the security requirements of the algorithm corresponding to the key pair.

The parameters and the algorithms used 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 Primary CA shall ensure the security of HSMs throughout its lifecycle.

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

6.2.2 Private key control

The Primary 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.

6.2.3 Private key escrow

Private keys are not escrowed.

6.2.4 Private key backup

Primary CA private keys are backed-up for recovery purposes either:

- outside of HSMs, but encrypted and with integrity controls. The encryption mechanism used provides a security level similar to storage inside the HSM itself, and uses an algorithm, a key length, and a usage mode supposed to resist cryptanalysis for at least the life duration of the protected private key. All private key backups of the Primary CA are stored inside a safe only accessible to persons in a Trusted Role.
- within an HSM with equivalent or greater security level. The HSM is operated in equivalent or greater security conditions.

Backups are made by a least two people in a Trusted Role.

6.2.5 Private key archival

The Primary CA private keys are not archived.

6.2.6 Private key transfer to or from a cryptographic module

The private keys of the Primary 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 mechanism ensuring that no sensitive information is transferred in a non-secure way. Each key's backup and restoration are performed by at least two persons in a Trusted Role in a secured area.

6.2.7 Private key storage in a cryptographic module

The private keys of the Primary CAs and Subordinate CAs are protected by the HSMs.

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

6.2.8 Method of activating private keys

Primary 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

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

6.2.10 Method of destroying private keys

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

6.2.11 Cryptographic Module Rating

Primary CA HSM: The HSM used by the Primary 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.

Subordinate CA HSM: The Primary CA does not provide the Subordinate CAs' HSMs. Subordinate CAs' HSM must meet the requirements defined in Appendix A.

6.3 Other aspects of key pair management

6.3.1 Public key archival

The Primary CAs and Subordinate CAs public keys are archived for at least 5 years after the expiry of the corresponding CA certificate. Archive conservation is described in section 5.5.

6.3.2 Certificate operational periods and key pair usage periods

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

6.4 Activation data

6.4.1 Activation data generation and installation

Generation and installation of the activation date corresponding to the Primary CA private key
The generation and the installation of the activation data of the Primary 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 is stored in personal, named smartcards. Each card is under the responsibility of the person it belongs to and is protected by secret data (PIN or Passphrase) or an equivalent mechanism known only by the cardholder. Smartcards are stored in individual safes when not in use. Each cardholder is responsible for safeguarding the card containing the activation data and must sign an agreement acknowledging these 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 Primary CA private keys shall be decommissioned using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of the private keys protected by such activation data.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

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

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

These security control mechanisms are described in this chapter.

Identification and authentication

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

Authentication 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:

The usage of utility tools is restricted and controlled. The administration and operating 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 equipment are documented in order to ensure the non-disclosure of sensitive information they may contain.

The set of sensitive hardware of the PKI has lifecycle-tracking procedures to ensure the traceability and maintenance procedures to ensure the availability of the functions and information. These procedures are documented. Personnel that need 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 Universign Primary CA is operated offline. Information transmission such as CRL transmission is performed through a mono-directional channel. Thus, this leads to a strict segmentation of its key certificate issuance systems from unrelated servers and systems. Moreover, the criticals components are placed in the securiest areas.

The network communications 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.

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

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

6.8 Timestamping

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

7 Certificate, CRL and OCSP profiles

7.1 Certificate profiles

All 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_[type]`[7]

Validity	30 years

Subject DN	C=FR,
	O=Cryptolog International,
	OU=0002 43912916400026,
	CN=`Universign_Primary_CA_[type]`[8]

Public Key	RSA 2048 bits

Certificate extension

Field	OID	Critical	Value
Subject Key Identifier	2.5.29.14	No	
KeyIdentifier			RFC 5280 - Method 1
Key Usage	2.5.29.15	Yes	
digitalSignature			False
nonRepudiation			False
keyEncipherment			False
dataEncipherment			False
keyAgreement			False
keyCertSign			True
cRLSign			True
encipherOnly			False
decipherOnly			False
Basic Constraint	2.5.29.19	Yes	
CA			True
Maximum Path Length			Absent

[7] `[type]` shall be replaced by `hardware` for Hardware Primary CA and by `software` for Software Primary CA

[8] `[type]` shall be replaced by `hardware` for Hardware Primary CA and by `software` for Software Primary CA

7.1.2 Subordinate 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_[type][9]

Validity	See Sect. 6.3.2
Subject DN	See Sect. 3.1
Public Key	See Sect. 6.1.5

[9] [type] shall be replaced by hardware for Hardware Primary CA and by software for Software Primary CA

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 [10]
CRL Distribution Points	2.5.29.31	False	
fullName			http://crl.universign.eu/universign_primary_ca_[type].crl[11]
reasons			Absent
cRLIssuer			Absent

With agreement from Universign, the Subordinate CA is allowed to add other extensions in accordance with [RFC 3647],such as Certificate Policy.

[10] This version of the CP/CPS is limited to path of length 0.

[11] [type] shall be replaced by hardware or software w.r.t. the condition met (see Appendix A)

7.2 CRL Profile

Base fields

Field	Value
Version	v2
Signature	RSA/SHA-256 [12].

Issuer DN	C=FR,
	O=Cryptolog International,
	OU=0002 43912916400026,
	CN=`Universign_Primary_CA_[type]` [13]

Next Update	This Update + 7 days

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 in accordance with [RFC 5280]

With the agreement of Universign, the Subordinate CA is allowed to add other extensions in accordance with [RFC 5280].

7.3 OCSP Profile

Not applicable.

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;

[12] or any stronger appropriate algorithm

[13] `[type]` shall be replaced by `hardware` for Hardware Primary CA and by `software` for Software Primary CA

- a [ETSI 319 411-1] 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-compliant items which might jeopardize the security of the service. Primary CAs commit to hiring 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 audits, the assessor is appointed by Universign, and is authorized to audit the practices relating to the component that is the subject of the audit. He or she may be part of Universign but is independent from the targeted Primary CA. For certification audits, the assessor must be independent and shall not have a conflict of interest that hinders his or her ability to perform an audit of the Primary CA.

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 Primary 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 Primary CA the result which can be "success", "failure" or "to be confirmed".

In case of failure, the assessment team delivers recommendations to the targeted Primary CA. The Primary 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 Primary CA confirms the compliance with the requirements of the CP/CPS.

8.6 Communication of results

The audit results of the Primary CA are made available to the qualification organism in charge of the certification of the Primary CA and of the Primary Trusted Parties.

9 Other business and legal matters

9.1 Fees

9.1.1 Certificate issuance or renewal fees

A Primary CA may charge Subordinate CAs for certificate issuance services.

9.1.2 Certificate access fees

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

9.1.3 Revocation or status information access fees

Primary CA LCRs publication services and revocation services are accessible free of charge. However, a Primary 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 Primary 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 Subordinate CAs, 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 is classified as confidential:

- private keys of the Primary CAs,
- activation data linked to the private keys of the Primary CAs,
- event journals,
- registration files (accepted and refused),
- audit reports,
- recovery, continuity and end of activity plans,
- cause of revocation of the certificates.

Other data can be classified as confidential, particularly if it is shown to be sensitive 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 (Primary CA certificates, CRLs, certificate information status,...) is not considered confidential.

9.3.3 Responsibility to protect confidential information

Universign processes confidential data in line with the current laws and regulations. Universign applies security procedures to protect the confidentiality of the assets listed in section 9.3.1.

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.

In particular

- The Primary CA ensures the confidentiality and the protection of data provided by the Primary Contacts;
- The Primary CA ensures to persons concerned by personal data process they can access, update or delete informations on request. The contact address is identifid in section 1.5.2;
- The Primary CA ensures its archives availability for legal and certification purposes (see Sect 9.4.6).

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 stated within this CP/CPS or in a agreement between a Primary CA and a Subordinate CA, a Primary CA shall not use the private data without authorisation, within 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 Subordinate CAs 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 Primary CAs keys belong to Universign. Subordinate CAs keys are the property of each Subordinate CA. Activation data of the Primary 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 Primary 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;
- adherance to the security principles for all the components of the PKI and their subsequent controls.

Unless the Primary CA can demonstrate it has not made any intentional or negligent error, the Universign Primary CA is responsible for damages caused to Relying Parties if:

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

9.6.2 RA representations and warranties

See above.

9.6.3 Subscriber representations and warranties

The Primary Contact of a Subordinate CA must:

- communicate correct and up-to-date information when requesting a Subordinate CA certificate;
- protect the private key under his or her responsibility;
- protect the access to the Subordinate CA certificate base;
- adhere to the conditions of use of the private key according to what is established in this CP/CPS;
- inform the Primary CA of any modification regarding the information contained in the Subordinate CA certificate;
- immediately perform a revocation request of a Subordinate CA certificate in case of suspected compromise of the corresponding private key.

The Primary Contact is registered with the Primary CA according to the process defined in this CP/CPS.

9.6.4 Relying party representations and warranties

Relying Parties using certificates from the Primary 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

Not applicable.

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

A Primary CA is allowed to ask a Subordinate CA for indemnities if the Subordinate CA does not respect the agreement with the Primary 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

On termination of this CP/CPS, PKI participants are still bound by the conditions of this CP/CPS for all certificates 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

Not applicable.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Not applicable.

9.16.5 Force majeure

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

9.17 Other provisions

9.17.1 Organization reliability

Universign ensures that 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.

A What is required of Subordinate CAs

This appendix presents the requirements for the Subordinate CAs. The organization operating a subscriber must ensure that the Subordinate CA complies with the following requirements:

1. The Subordinate CA shall issue X.509 v3 certificates;
2. The Subordinate CA shall write its own CP and its own CPS describing its PKI operation, in accordance with requirements of this Appendix;
3. The Subordinate CA shall comply with at least one of the following standard (or equivalent accepted by Universign):
   - ETSI EN 319 411-1 [**ETSI 319 411-1**];
   - ETSI EN 319 411-2 [**ETSI 319 411-2**].
4. The Subordinate CA shall perform an annual audit to provide evidence of compliance with the above standards. The results of the audit shall be transmitted to Universign.
5. The Subordinate CA shall have a Primary Contact at all times. This Primary Contact shall be explicitly nominated and shall have the authority to perform operations relative to certificate lifecycle (request, revocation,...). If the Primary Contact changes, the Subordinate CA shall notify Universign immediately and shall provide a new Subordinate CA as soon as possible.
6. The Subordinate CA shall generate and use private keys in a device in line with the following (or a device that meets equivalent or stronger requirements):
   - FIPS 140-2 Level 3; or
   - Common Criteria ISO/CEI 15408 EAL4+ or greater (Protection Profile CWA 14167-2 or CWA 14167-3) ;
7. The Subordinate CA shall use RSA 2048-bit private keys (or stronger) and has an algorithm of SHA-2 family (256/384/512) or stronger.
8. The Subordinate CA shall use key generation devices with parameters that respect security requirements w.r.t. the algorithm and the key used. Parameters and signature algorithms used shall be described in their PC.
9. The Subordinate CA shall issue certificates for RSA 1024-bit (or stronger or equivalent) private keys.

10. if the Subordinate CA certificate is an *Hardware Certificate* (OID: 1.3.6.1.4.1.15819.5.1.2.1), private keys associated with the certificate issued by Subordinate CA shall be generated and used in a secure device that meets the following:

    - FIPS 140-2 Level 2 or greater; or
    - Common Criteria ISO/CEI 15408 EAL4+ or greater (Protection Profile CWA 14169 or certified as conforming to Protection Profile Secure Signature Creation Device (SSCD) by an official European entity);

11. Subordinate CAs shall never deliver a certificate with an expiration date greater than the one of its private keys.

12. If the Subordinate CA is not operated in Universign secured premises by Universign personnel, the Subordinate CA shall be operated in equivalent or greater security conditions. Universign *may* organize a security audit or ask for an independent audit of the premises and practices of the Subordinate CA to ensure that a sufficient security level is met;

13. The Subordinate CA shall notify Universign without delay if:

    - a private key is lost, compromised, or suspected of being compromised;
    - control of the private key is lost (due to the activation data being lost or compromised, for example);
    - the information regarding a Subordinate CA included in the certificate is no longer accurate;
    - there is a major intrusion or suspicion of major intrusion within the Subordinate CA's information system.
    - a major change occurs in the PC.

14. If its private key is compromised, a Subordinate CA shall without delay perform a revocation request and shall no longer use its private key to issue new certificates.

B Primary Trusted Parties

Universign maintains a list of Primary Trusted Parties for each primary Primary CA. The Primary Trusted Parties are individuals or entities with a high degree of implication in the UTN or, due to their status, which have a specific relationship with Universign. They are notified each time a major event happens within the Primary CA lifecycle.

B.1 Origin of the Primary Trusted Parties

There is no strict definition of Primary Trusted Parties. Primary Trusted Parties are Relying Parties that are considered by Universign as Primary Trusted Parties. Their activities are highly dependent on their trust of the UTN. Primary Trusted Party may be (but not limited to):

- Software companies with a trusted certificate store;
- The owners of a Trust-Service Status List (TSL);
- Government bodies;
- Auditors.

B.2 How to become a Primary Trusted Party

Being added to the list of Primary Trusted Parties can occur either:

- following acceptation of a motivated request;
- following an invitation from Universign.

Motivated Request Any Relying Party can request to become a Primary Trusted Party. The process is as follows:

- The Relying Party sends a request to the contact identified in Section 1.5.2. This request shall contain at least:
  - The name of individual or entity to subscribe;
  - Motivations;
  - Name and email address of the contact.
- The Universign Approval Board validates the request. Universign takes reasonnable measures to ensure the origin of the request. Universign *may* refuse a request if Universign considers this request as not relevant. Universign processes requests in a reasonable timeframe.

Invitation The Universign Approval Board can invite individuals or organizations to join the Primary Trusted Parties list. If the individual or organization responds positively and if Universign has all the necessary information, Universign adds the individual or organization to the list.

B.3 How to unsubscribe

Someone on the Primary Trusted Parties list can unsubscribe at any moment on request. Universign checks that the origin of the request is the provided contact point before deleting someone from the list. Universign can decide to delete someone from the list. Causes of deletion may be (but not limited to):

- invalid contact address;
- contract or relation between the Primary Trusted Party and Universign ended or has changed significantly.

Primary Trusted Parties are responsible for maintaining at least one contact at any moment. If an entity no longer has a contact, Universign will try to contact the entity using reasonable means, but has no obligation to succeed in contacting the entity.

B.4 Events notified to Primary Trusted Parties

Primary Trusted Parties are notified, *via* their contact registered by Universign, when one of the following events occurs:

- issuance of a new Subordinate CA certificate by a Primary CA;
- revocation of a Subordinate CA certificate by a Primary CA;
- the key of a Subordinate CA or a Primary CA is compromised;
- a major intrusion in the information system of a Primary CA or of a Subordinate CA;
- a major modification of this CP/CPS or of a Subordinate CA.

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^{o}78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n^{o}2004-801 du 6 août 2004.