Certification Practice Statement

Universign CA Hardware

Universign

7, rue du Faubourg Poissonnière, 75009 Paris, France

OID: 1.3.6.1.4.1.15819.7.1.3

VERSION : 2.6	DIFFUSION : PUBLIC	Effective date : 15/05/2019

Contents

1 Introduction

1.1 Overview

This Certification Practice Statement defines the implementation of the commitments made by Universign, member of the UTN, for the issuance and management of electronic Certificates by the CA *Universign CA Hardware*.

1.1.1 Presentation of the Universign Trust Network

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

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

The UTN particularly comprises:

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

1.1.2 Organisation of the Universign Trust Network

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

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

The UTN:

- publishes the Certification Policy governing the CAs;

- publishes the Timestamping Policy governing the TSAs;
- manages the Primary CAs of the network.

The members of UTN:

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

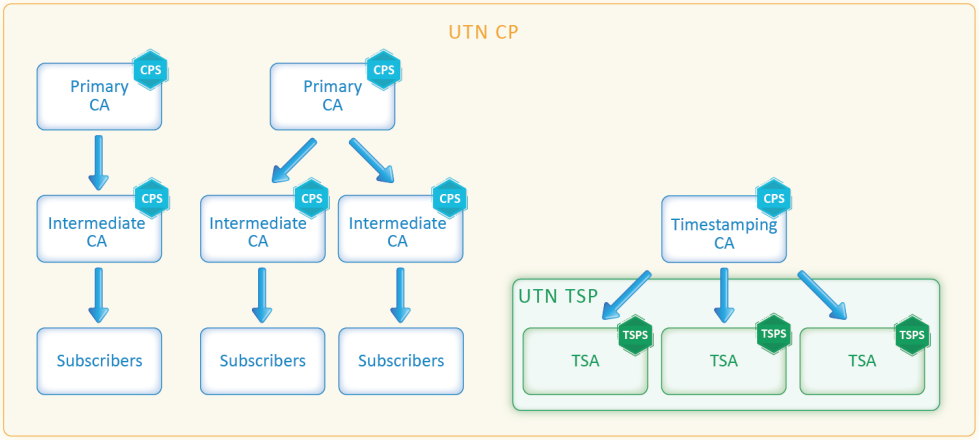


Figure 1: Organisation of the UTN

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

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

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

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

The UTN may delegate all or some of its functions.

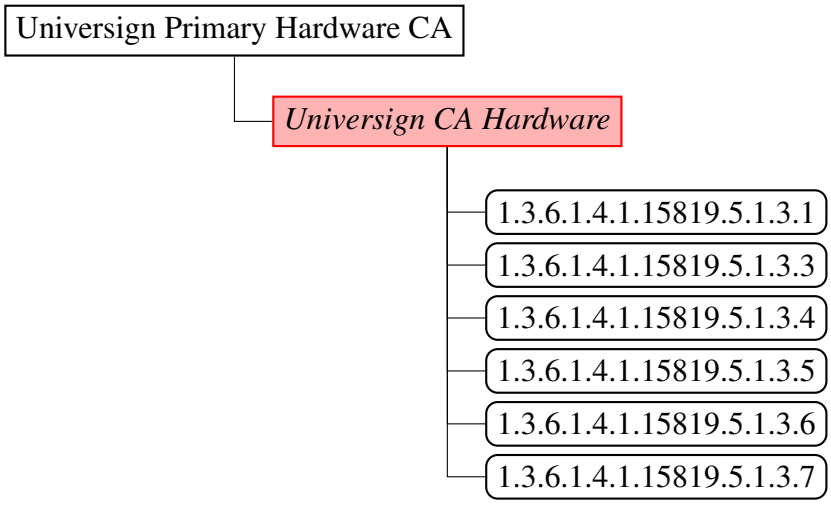
1.2 Document name and identification

This document is the Certification Practice Statement of the CA *Universign CA Hardware*, operated by Universign, and acting in the capacity of Intermediate CA within the UTN.

This CPS defines the procedures that are effectively implemented by the CA to issue and manage Certificates according to the commitments defined in the CP of the UTN.

The OID assigned to this document is: 1.3.6.1.4.1.15819.7.1.3

Within the hierarchy of the UTN, this CA (*Universign CA Hardware*) issues Certificates that comply with the OIDs defined by the CP of the UTN, as summarised below:



1.3 UTN participants

1.3.1 Certification Authorities

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

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

- define and approve the Certification Practice Statement of the CA (CPS) in accordance with this CP;

- define the process for updating the CPS;
- inform the UTN about and provide it with the CPS and its revisions.

1.3.2 Registration Authorities

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

1.3.3 Subscribers

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

1.3.4 Timestamping Authorities

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

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

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

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

1.3.5 Relying parties

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

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

1.3.6 Certificate Officer

A Certificate Officer is a natural person who:

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

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

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

1.4 Certificate usage

1.4.1 Appropriate Certificate uses

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

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

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

- signing documents with an electronic signature (for natural person Certificates issued by an Intermediate CA);

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

1.4.2 Prohibited Certificate uses

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

1.5 Policy administration

1.5.1 Organization administering the document

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

contact@universign.com

1.5.2 Contact person

Any questions related to this document may be addressed to:

The Approval Board
Universign
7, rue du Faubourg Poissonnière, 75009 Paris, France

contact@universign.com

1.5.3 Person determining CP suitability for the policy

The UTN determines the appropriateness of a CPS as regards the CP.

1.5.4 CPS approval procedures

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

1.6 Definitions and acronyms

The terms used in this document are as follows:

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

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

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

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

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

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

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

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

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

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

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

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

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

Timestamping Practice Statement (TSPS) Refers to the practices (organisation, operating procedures, technical and human resources) applied by the TSA to implement its timestamping service. These practices are compliant with the TSP (s) that the TSA has pledged to comply with.

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

2 Publication and repository responsibilities

2.1 Repositories

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

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

2.2 Published information

The CA pledges to inform the Subscribers and the Relying Parties about:

- the CP applicable to the Certificates that they use;
- the terms of use of the certification service;
- the CPS related to the applicable CP;
- the CRLs published in accordance with the requirements of the CP applicable to the Certificates;
- the currently valid Certificates of the CA.

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

The CA publishes the information defined in section 2.2 on the UTN 's publishing website. It transmits this information to the UTN in timeframes that are compatible with section 2.3.

2.3 Time and frequency of publication

The time and frequency vary according to the information concerned:

- The CRLs are published every hour for Intermediate CAs and every day for the Primary CAs.
- The CA Certificates are distributed or uploaded before use.
- The CP, CPS and Relying Party Agreement are published after every update.

2.4 Access Controls on repositories

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

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

3 Identification and Authentication

3.1 Naming

3.1.1 Types of names

The names used are compliant with the specifications of standard X.500.

The CA and the Subscriber are identified by an explicit name: the "Distinguished Name" ("DN " hereinafter) of type X.501. The DN fields and their semantics are given in the table below.

Natural person Certificates Natural person Certificates issued by the CA contain the following fields in the DN:

Field	Mandatory	Field Semantic	Verified by the RA	Document used for verification
C	Yes	Nationality of the CA		
givenName	Yes	Given name of the natural person	Yes	ID proof that is valid at the time of the application
surname	Yes	Surname of the natural person	Yes	ID proof that is valid at the time of the application
O	No	Designation of the legal person to which the natural person is linked	Yes	Official identification document of the legal person and signed mandate
OI	No	Legal unique identifier of the legal person to which the natural person is linked, structured as per ETSI 319 412-1	Yes	Official identification document of the legal person and signed mandate
SERIALNUMBER	Yes	The serial number assigned by the RA	Yes [1]	
CN	Yes	Usual given name and surname of the natural person	Yes	ID proof that is valid at the time of the application

Legal person Certificates Legal person Certificates issued by the CA contain the following fields in the DN:

[1] It will only be verified that this number is unique.

Field	Mandatory	Field Semantic	Verified by the RA	Document used for verification
C	Yes	Country of establishment of the Subscriber	Yes	Identification document of the legal person.
ST	No	State/Region of the Subscriber	Yes	Identification document of the legal person.
L	No	City of the Subscriber	Yes	Identification document of the legal person.
O	Yes	Legal name of the Subscriber	Yes	Identification document of the legal person.
OI	Yes	Legal unique identifier of the Subscriber, structured as per ETSI 319 412-1	Yes	Identification document of the legal person.
CN	Yes	Free named referring to the organization	Yes [2]	

3.1.2 Need for names to be meaningful

The names chosen to designate the Certificate Subscribers must be meaningful, and must allow directly or indirectly identifying the Certificate Subscriber.

3.1.3 Anonymity or pseudonymity of Subscribers

The anonymity or pseudonymity of Subscribers is forbidden.

3.1.4 Rules for interpreting various name forms

No specific commitment.

3.1.5 Uniqueness of names

The same DN cannot be assigned by a CA to different Subscribers.

The RA ensures the uniqueness of the DNs by following the conditions defined by the registration process (see 3.2.2).

The CA generates a unique serial number for every registration file corresponding to an application for a natural person Certificate. This unique serial number is entered in the SERIALNUMBER field of the Certificate 's DN.

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

The CA enters a unique identifier in the `OI` field of the legal person Certificates that it issues, which corresponds to an enrolment, registration or record number in a national repository or register.

3.1.6 Recognition, authentication, and role of trademarks

The Subscribers declare that they possess the intellectual property rights associated with the names, brands, domain name or any other distinctive sign contained in their Certificate. The CA does not carry out any verification of these rights, but is still authorised to reject a Certificate application or to revoke a Certificate in case of a dispute regarding these distinctive signs. The CA cannot be held liable in the event of an unauthorised use of elements protected by intellectual property rights.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

If it generates its keypair, a Subscriber must prove to the CA issuing the Certificate, by appropriate means, that it is indeed in possession of the private key corresponding to the public key to be certified.

The proof of possession is obtained:

- either by signing the certificate application in the PKCS#10 format (or another mechanism accepted by the CA providing equivalent assurance) using the Subscriber 's private key;
- or by sending an application through a service that is recognised and accepted by the CA managing the Subscriber 's key pair.

3.2.2 Authentication of organization identity

The identity of the Certificate Officer of the legal person is verified by the RA:

- during a face-to-face meeting for Certificates issued under OID 1.3.6.1.4.1.15819.5.1.3.5 or 1.3.6.1.4.1.15819.5.1.3.7 or Intermediate CA Certificates.
- without an obligation to meet face-to-face for Certificates issued under OID 1.3.6.1.4.1.15819.5.1.3.4.

The applicant shall provide the following information:

- a national identity proof of the future Certificate Officer bearing an identity photograph, specifying the date and place of birth, and still valid at the time of submitting the application;

- an email address and/or mobile number allowing the CA to contact the Certificate Officer;
- a mandate, signed and dated less than 3 months in the past by a legal representative of the entity, appointing the future officer to whom the Certificate is to be issued. This mandate must be signed to signify acceptance of the future officer.
- a legal document bearing proof of the existence of the organisation, valid at the time of submission of the Certificate application (e.g. a company registration certificate dated less than 3 months in the past). The document must bear the legal unique identifier number of the legal person in question.

3.2.3 Authentication of individual identity

The identity of the future Subscriber is verified by the RA. This verification is conducted:

- during a face-to-face meeting for Certificates issued under OID 1.3.6.1.4.1.15819.5.1.3.1 or 1.3.6.1.4.1.15819.5.1.3.6.
- without an obligation to meet face-to-face for Certificates issued under OID 1.3.6.1.4.1.15819.5.1.3.3.

The applicant shall provide the following information:

- a national identity proof bearing an identity photograph, specifying the date and place of birth, and still valid at the time of submitting the application;
- an email address and/or mobile number personally assigned to the Subscriber.

3.2.4 Non-verified Subscriber information

Information that is not verified by the RA is specified in section 3.1.1.

3.2.5 Validation of authority

The RA verifies the authorisation of a natural person to represent a legal person during the validation of the Subscriber 's identity.

The Certificate Officer is authorised to represent the Subscriber through a signed mandate of the legal representative of the legal person. The mandate is provided and verified during the registration (see Section 3.2.3).

3.2.6 Criteria for interoperation

Not applicable.

3.3 Identification and authentication for re-key requests

The keys associated with the Certificates are not renewed.

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 RA authenticates the revocation applicant, mainly on the basis of the information contained in the registration file in the case of a revocation application of a Certificate intended for a natural person. It also verifies the applicant's authorisation in accordance with section 4.9.2 in case of a revocation application of a Certificate intended for a legal person.

Natural person Certificate a revocation application can be filed in the following manner:

- through the interface of the CA's revocation service, after authenticating the Subscriber;
- in case of loss of password, via a specific service accessible to all Certificate Subscribers. The CA authenticates the applicant (e.g. by using the information in the registration file) and then, if successful, revokes the Certificate.

Legal person Certificate a revocation application can be filed in the following manner:

- through the interface of the revocation service, after authenticating the Certificate Officer.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate application

4.1.1 Who can submit a Certificate application

The Certificate application is sent by the Subscriber or by a person expressly appointed by the Subscriber (i.e. the prior consent of the future Subscriber is compulsory).

Natural person Certificate: the applicant files the Certificate application by filling a registration application form. The applicant is the Subscriber.

Legal person Certificate: the applicant files the Certificate application by filling the registration application form. The applicant is the Certificate Officer.

4.1.2 Enrolment process and responsibilities

The Certificate application includes identification data on the Subscriber. This identification data is transmitted under its sole responsibility.

The registration process at the CA requires the following steps:

- The applicant reads and accepts the CA 's Subscriber Agreement;
- the applicant provides the required information during the registration application. In this respect, he/she guarantees the accuracy of the provided information and must provide the RA with all information required for the registration file;
- the RA validates the information of the registration file (see Section 3.2.3) and transmits it securely to the CA;
- the applicant generates (or requests the generation of) its dual-key in a cryptographic device that complies with the requirements of Section 6.2.11;
- the applicant transmits (or requests the transmission of) its public key to the CA;
- the applicant proves to the CA that it possesses and/or controls its private key in accordance with section 3.2.1.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

The RA validates the Certificate applications from the Subscribers. The RA validates the information provided by the Subscribers in accordance with the provisions of section 3.2.

4.2.2 Approval or rejection of Certificate applications

The CA processes the application on receiving it. If the application is rejected during one of these steps, the applicant is informed of this as soon as possible.

The procedure for the validation of a Certificate application by the RA is as follows:

- the RA verifies that the registration file is complete and valid. In particular, the RA verifies the compliance of the information in the registration application with the supporting documents provided by the applicant;
- the RA successfully identifies the applicant and the provided information in accordance with section 3.2.

4.2.3 Time to process Certificate applications

A Certificate application remains valid until it is rejected. There is no maximum duration for the issue of a Certificate.

4.3 Certificate issuance

4.3.1 CA actions during Certificate issuance

The CA creates a Certificate once the validation process of the Certificate application is complete, as defined in section 4.2. The issued Certificate is compliant with the information contained in the Certificate application and with the profile defined in section 7.1.

The CA verifies the Certificate 's compliance with the data and proof contained in the registration file.

4.3.2 Notification to Subscriber by the CA of issuance of Certificate

The CA notifies the applicant within a reasonable period about the issue of the Certificate and provides it in an appropriate manner.

There are no special notifications on the issue of the Certificate.

4.4 Certificate acceptance

4.4.1 Conduct constituting Certificate acceptance

The Certificates are deemed as accepted if no objection is made within 48 hours after its provision or at the first use of the associated private key.

The following facts are deemed as acceptance by a Subscriber of the Certificate issued by the CA:

- downloading of the Certificate by the Subscriber or downloading of a message containing the Certificate constitutes an implicit acceptance of the Certificate;
- no objection filed on the contents of the Certificate within a period of 48 hours after the issue of the Certificate.

4.4.2 Publication of the Certificate

The Certificates are public.

4.4.3 Notification of Certificate issuance by the CA to other entities

Not applicable.

4.5 Keypair and Certificate usage

The Subscriber pledges to use the Certificate in accordance with:

- the CP, especially for the limits of use defined in section 1.4;
- the Subscriber Agreement that it consented to;
- the special terms and conditions defined between the CA and the Subscriber, where applicable;
- the KeyUsage extension or any other extension restricting the use of the key, defined in the issued Certificate.

The Relying Parties consent to the terms and conditions of the Relying Party Agreement before any use of the Certificates of UTN.

The Relying Parties are required to:

- determine that the use of the Certificate is compliant with the conditions defined in the CP (see section 1.4);

- determine that the Certificate is used in compliance with the KeyUsage extension defined in it;
- verify the status of the Certificate.

The CA cannot be held liable in case of any use of the Certificate that does not comply with the CP, the Subscriber Agreement, the Relying Party Agreement or any other special agreement signed between the CA and the Subscriber.

4.6 Certificate renewal

No renewal is authorised.

4.6.1 Circumstance for certificate renewal

Not applicable.

4.6.2 Who may request renewal

Not applicable.

4.6.3 Processing certificate renewal requests

Not applicable.

4.6.4 Notification of new certificate issuance to Subscriber

Not applicable.

4.6.5 Conduct constituting acceptance of a renewal certificate

Not applicable.

4.6.6 Publication of the renewal certificate by the CA

Not applicable.

4.6.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.7 Certificate re-key

Certificate re-key is not allowed.

4.7.1 Circumstance for certificate re-key

Not applicable.

4.7.2 Who may request certification of a new public key

Not applicable.

4.7.3 Processing certificate re-keying requests

Not applicable.

4.7.4 Notification of new certificate issuance to subscriber

Not applicable.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Not applicable.

4.7.6 Publication of the re-keyed certificate by the CA

Not applicable.

4.7.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.8 Certificate modification

No modification of the Certificate is authorised without renewal.

An application to modify a Certificate results in its revocation, followed by the filing of a new initial application.

4.8.1 Circumstance for certificate modification

Not applicable.

4.8.2 Who may request certificate modification

Not applicable.

4.8.3 Processing certificate modification requests

Not applicable.

4.8.4 Notification of new certificate issuance to Subscriber

Not applicable.

4.8.5 Conduct constituting acceptance of modified certificate

Not applicable.

4.8.6 Publication of the modified certificate by the CA

Not applicable.

4.8.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

The Certificate may be revoked in case of:

- a request from the Subscriber;
- non-compliance with the Subscriber Agreement;
- inaccuracy or nullity of the information of the Certificate or if this information infringes upon the rights of a third party;
- suspicions of a private key being compromised, lost or stolen (including one of the private keys of the CA);
- error in the registration procedure;
- termination of the contractual relations between the CA and the Subscriber;
- non-payment related to the certification service, if applicable;

- permanent cessation of the CA 's activity;
- loss of control of the private key associated with the Subscriber 's Certificate (loss or theft of the activation data of the private key);
- use of the Certificate that damages or is likely to damage the CA.

The CA does not publish the causes for revocation.

4.9.2 Who can request revocation

Only the Subscriber, the Certificate Officer and the CA are authorised to file an application for the revocation of a Certificate.

Natural person Certificate: Individuals who can request for the revocation of a Certificate of a natural person are as follows:

- the manager of the CA, or if he is absent and if it is urgent, the Approval Board;
- the Subscriber.

Legal person Certificate: Individuals who can request for the revocation of a Certificate of a legal person are as follows:

- the manager of the CA, or if he is absent and if it is urgent, the Approval Board;
- the Subscriber;
- the Certificate Officer.

4.9.3 Procedure for revocation request

The validation of the application by the CA must include the verification of the origin of the application and its admissibility. The CA authenticates the revocation application in accordance with the provisions of section 3.4 and revokes the Certificate immediately. All operations are conducted in such a way as to guarantee the integrity, confidentiality (if necessary) and authenticity of the data processed during the process. The CA informs the revocation applicant and the Subscriber (if they are two different persons) about the effective revocation of the Certificate and the change in status. All revocations are irrevocable.

Natural person Certificate: This application can be formulated as indicated in section 3.4:

- via the user interface of the service, available at the address https://app.universign.com/fr/revocation/
- via a specific service accessible to Subscribers;
- by email.

Legal person Certificate: This application can be formulated as indicated in section 3.4:

- via the user interface of the service;
- by email.

Specificities for revocation applications sent by electronic messaging services The applicant transmits a revocation application that must contain the following information:

- the identifier of the Subscriber (see Sect. 3.1.1);
- information allowing the CA to securely identify the Certificate to be revoked;
- possibly, the cause of the revocation. This information is given for information purposes only and does not appear in the CRL.

4.9.4 Revocation request grace period

The revocation application is to be sent to the CA as soon as the Subscriber becomes aware of one of the possible causes of revocation. It must be filed immediately

4.9.5 Time within which CA must process the revocation request

Revocation applications are processed immediately after effectively authenticating the applicant and accepting the application, and within a maximum period of 24 hours.

4.9.6 Revocation checking requirements for Relying Parties

The Relying Parties are required to verify the status of the Certificates and the corresponding chain of trust.

4.9.7 CRL issuance frequency

The CRLs are updated at least once every 60 minutes.

4.9.8 Maximum latency for CRLs

CRLs are published within a maximum period of 30 minutes after they are generated.

4.9.9 On-line revocation/status checking availability

The Certificate revocation and status service is available on a publishing website. The Certificate status information system may include one or more OCSP responders (online certificate status protocol). The CA indicates in its Certificates that it issues a link to the OCSP responder to be used to verify the status of the Certificate. Under normal operation, OCSP responders are available 24/7.

4.9.10 On-line revocation checking requirements

A Relying Party is required to verify the status of a Certificate before using for verifying an electronic signature or seal. The Relying Party may either check the most recently published CRL or file a request for the Certificate status with the OCSP responder.

4.9.11 Other forms of revocation advertisements available

Not applicable.

4.9.12 Special requirements regarding key compromise

If the private key of the CA is compromised or suspected of being compromised, the CA informs the participants of UTN of the harmful effects of such an incident by appropriate means.

4.9.13 Circumstances for suspension

The suspension of Certificates is not authorized.

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 CA must provide the Relying Parties with information on the status of Certificates, allowing them to verify and validate them prior to use. The CA ensures the integrity and authenticity of the published CRLs and OCSP responses. The CRLs and OCSP responses contain information on the status of the Certificates until their expiry. The information on the status of qualified Certificates are preserved even after their expiry.

The CRLs and the links to the OCSP responder(s) are published on a specific publishing website that is publicly accessible:

- from the address defined in Section 2.1;
- from the address specified in the issued Certificates.

4.10.2 Service availability

The function of information on the status of Certificates is available on multiple publishing servers, thereby ensuring 24/7 availability under normal operating conditions.

4.10.3 Optional features

Not applicable.

4.11 End of subscription

The end of relations between the CA and a Subscriber is defined in a contract. The contract between the CA and the Subscriber may define obligations that persist after the expiry or revocation of the Certificate. If such a clause is not present, the relations end at the expiry or revocation of the Certificate.

4.12 Key escrow and recovery

The 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

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

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

5.1 Physical controls

5.1.1 Site location and construction

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

- The first data centre is certified SSAE16/ISAE3402 SOC-1, ISO 27001, PCI-DSS, FACT, ISO 9001, ISO 50001.
- The second data centre is certified ISO 9001:2008, ISO/IEC 27001:2005 and ISO 14001.

5.1.2 Physical access

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

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

Physical access is restricted by the implementation of access control mechanisms protecting the highly secure zones of the host. Access to these rooms is reinforced by biometric access control. The access profiles to each zone are defined and maintained by the CA. The secure zones of the secure premises and sites of the CA are regularly inspected to verify that the access control systems are still operational. Supervision and logging systems are implemented on all sites with secure zones. Access controls are applied to all secure zones.

A logbook is filled out at every maintenance operation conducted on the equipment of the CA. This logbook contains at least the following information:

- start date and time of the intervention;
- surname and first name of the intervening staff;
- description of the intervention conducted;
- end date and time of the intervention;
- signature of the intervening staff.

5.1.3 Power and air conditioning

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

The measures taken are:

- Redundancy of the power supply circuits: N+1
- Redundancy of the cooling system: N+1 (for the coolers) and N+2 (for the room air-conditioning units)

5.1.4 Water exposures

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

The data centres are located outside of flood zones. Water leakage detection systems have been installed.

5.1.5 Fire prevention and protection

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

- The first main one has a fire protection system: detection system, water sprinkler extinguishing system.
- The second data centre has a Siemens category A fire safety system and an automatic inert gas-based fire extinguishing system.

5.1.6 Media storage

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

5.1.7 Waste disposal

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

In particular, the following destruction measures are applicable.

- The paper medium / CD / smart cards are destroyed before being scrapped.
- HSMs are uninstalled (reset) and, if necessary, made unusable as per the manufacturer's recommendations.
- Storage media is rendered illegible by appropriate methods before being scrapped.

5.1.8 Off-site backup

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

5.2 Procedural controls

5.2.1 Trusted roles

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

The following Trusted Roles have been defined:

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

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

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

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

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

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

Registration operator : he carries out all registration operations of future Certificate Subscribers.

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

5.2.2 Number of persons required per task

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

5.2.3 Identification and authentication for each role

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

Every assignment or revocation of a Trusted Role is subject to a form and a defined procedure. An inventory of the Trusted Roles is kept up to date. The Trusted Roles are reviewed at least once a year.

5.2.4 Roles requiring separation of duties

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

Keeping an inventory of the Trusted Roles helps to ensure that the same person does not have multiple incompatible roles.

5.2.5 Risk analysis

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

The risk analysis of the CA is conducted using the Ebios method. Its relevance is evaluated at least once every two years and is subjected to an update when necessary.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

The CA ensures that the assignments of staff to Trusted Roles correspond to their professional skills. The supervisory staff possesses the appropriate expertise and is familiarised with the security procedures. Anyone intervening in Trusted Roles is informed of his responsibilities (job description) and the procedures related to

system security and staff control. Staff occupying Trusted Roles are appointed by the management of the CA.

5.3.2 Background check procedures

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

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

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

These verifications are conducted by the CA in compliance with the regulations in force and prior to assigning a Trusted Role. They are reviewed at least once every 3 years.

5.3.3 Training requirements

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

5.3.4 Retraining frequency and requirements

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

A continuous training plan is developed. It is evaluated and reviewed annually.

5.3.5 Job rotation frequency and sequence

Not applicable.

5.3.6 Sanctions for unauthorized actions

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

5.3.7 Independent contractor requirements

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

5.3.8 Documentation supplied to personnel

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

5.4 Audit logging procedures

5.4.1 Types of events recorded

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

- all events related to the registration (certificate application);
- all events related to the life cycle of the CA 's keys;
- all events related to the life cycle of the certificates issued by the CA, including events linked to the revocation;
- all events of the various components of the CA (start-up of servers, network access, etc.).

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

5.4.2 Frequency of processing log

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

The event logs are checked once every working day, in order to identify anomalies related to failed attempts.

The logs are analysed in full whenever an anomaly is detected and at least once every week.

A reconciliation between the different event logs of functions that interact between themselves (registration authority and generation function, function of managing revocations and function of providing information on certificate statuses) is conducted once a month.

5.4.3 Retention period for audit log

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

The event logs are stored on site for a minimum duration of one month. The event logs are outsourced every month for archiving by the CA for the duration required for providing evidence in administrative and legal proceedings, in accordance with the applicable law.

5.4.4 Protection of audit log

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

5.4.5 Audit log backup procedures

The logs are regularly backed up on an external system.

The external backup of event logs is saved daily.

5.4.6 Audit collection system

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

The event logs are preserved for 7 years. The evidence files containing data from event logs are preserved according to the applicable contractual requirements and for a maximum duration of 99 years.

5.4.7 Notification to event-causing subject

There is no notification of events.

5.4.8 Vulnerability assessments

The CA implements controls for detecting:

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

The CA implements the following controls:

- daily control of physical access to the operating rooms;
- daily control of CRL publications;
- daily analysis of events and backups of the CA. All events are then analysed by persons having Trusted Roles;
- security tests (vulnerability scans, intrusion tests) and regular reports.

5.5 Records archival

5.5.1 Types of records archived

The following data is archived:

- the CPS;
- the published CRLs and Certificates;
- the Subscribers ' registration data;
  - proof of acceptance of the general and special terms and conditions of use and/or the Subscriber Agreement (see Section 4.1.2);
  - the Subscribers ' registration applications;
  - a copy of the information that enabled verifying the identify of a natural person;
  - the registration file of Subscribers (see section 3.2);
- the event logs, particularly containing:
  - events related to a significant change in the CA 's environment and the specific time of occurrence of the event;

- events related to operations on the keys and certificates issued by the CA and the specific time of occurrence of the event.

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

5.5.2 Retention period for archive

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

Certificate application forms : The Certificate application forms are preserved for 17 years after the Certificate is issued, and for 1 year after an application is rejected.

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

Event logs : The event logs are archived for up to 7 years after the expiry of the last Certificate issued by the CA.

5.5.3 Protection of archive

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

5.5.4 Archive backup procedures

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

5.5.5 Requirements for time-stamping of records

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

5.5.6 Archive collection system

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

5.5.7 Procedures to obtain and verify archive information

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

5.6 Key changeover

The CA does not have an automatic key renewal procedure; instead, a CA must generate a new keypair and file a Certificate application with a Primary CA before the expiry of the currently valid CA Certificate.

The CA must apply all necessary actions to prevent any interruption of the CA 's operations.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

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

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

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

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

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

This recovery plan is tested once a year.

5.7.3 Entity private key compromise procedures

This point is covered in the business recovery and continuity plans. The compromising of a key of the CA immediately triggers the revocation of the issued Certificates. In this case, the various persons and entities concerned are informed of the unsafe nature of the CRL signed by the compromised key of the CA. Similar

measures are taken if the soundness of the algorithm used or that of the parameters used by the CA become insufficient for the purposes of the CA.

5.7.4 Business continuity capabilities after a disaster

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

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

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

The Business Recovery Plan is tested regularly.

5.8 CA termination

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

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

This plan is verified and updated regularly.
This plan is updated and reviewed annually.

6 Technical security controls

6.1 Keypair generation and installation

6.1.1 Keypair generation

The keys of the CA are generated:

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

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

The Subscribers ' keypairs to be certified are generated in accordance with the requirements of sections 6.1.5 and 6.1.6.

The public keys of the Subscribers are transmitted to the CA under the conditions laid down in section 6.1.3.

6.1.2 Private key delivery to Subscriber

Not applicable.

6.1.3 Public key delivery to CA

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

6.1.4 CA public key delivery to Relying Parties

The CA 's Certificate is published on the Publishing Website.

The Certificate contains the information specified in chapter 7 of the CP.

6.1.5 Key sizes

The CA 's keys must be compliant with (or cryptographically superior or equal to) the following characteristics:

Certificate	Key Size	Format

CA	2048 4096 (for keys generated after 1 January 2019)	RSA RSA

The Subscribers ' keys must be compliant with (or cryptographically superior or equal to) the following characteristics:

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

6.1.6 Public key parameters generation and quality checking

The CA and the Subscribers must use certified hardware (see Sect. 6.2.11)) and algorithms whose parameters comply with the appropriate security standards. The parameters and algorithms used are documented in chapter 7.

6.1.7 Key usage purposes

See section 7.1.

6.2 Private key protection and cryptographic module engineering controls

6.2.1 Cryptographic module standards and controls

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

- ensuring their integrity during their transport from the supplier;
- ensuring their integrity during their storage before the key ceremony;
- ensuring that the operations of activation, backing up and restoration of the signature keys are conducted under the control of two staff members having Trusted Roles;

- ensuring that they are in a proper functional state;
- ensuring that the keys that they contain are destroyed after being decommissioned.

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

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

6.2.3 Private key escrow

The private keys are not escrowed.

6.2.4 Private key backup

The private keys of the CA are backed up via copies:

- either outside an cryptographic module but in an encrypted form and with an integrity control mechanism. The corresponding cryptographic offers a security level equivalent to storage in a cryptographic module and is based on an algorithm, a key length and a standard operating procedure capable of resisting cryptanalysis attacks for at least the service life of the thus protected key. These backup copies of the CA 's private keys are stored in a secure safe that can be accessed only by persons with Trusted Roles.
- or in an equivalent cryptographic module operated under similar or superior security conditions.

The backups are made under the control of two persons having Trusted Roles.

6.2.5 Private key archival

The private keys of the CA are not archived.

6.2.6 Private key transfer into or from a cryptographic module

Apart from the backup copies, the private keys of the CA are generated in its cryptographic module and hence are not transferred. During the generation of a backup copy, the transfer implements an encryption mechanism that enables guaranteeing that no sensitive information transits in an unsecure manner.

6.2.7 Private key storage on cryptographic module

The private keys of the CA are stored in a cryptographic module. For the purposes of backup copies, they are stored in a cryptographic module in compliance with the measures defined in section 6.2.4.

6.2.8 Method to activate the private key

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

6.2.9 Method to deactivate the private key

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

6.2.10 Method to destroy the private key

The private key of the CA is destroyed from its cryptographic module. The CA ensures that all corresponding backup copies are also destroyed.

6.2.11 Cryptographic Module Rating

Cryptographic module of the CA: The cryptographic module used by the CA complies with the following certification requirements:

- EAL 4+ as regards the Common Criteria of ISO/CEI 15408 (compliant with the Protection Profile CWA 14167-2 or CWA 14167-3); or
- FIPS 140-2 level 3
- or equivalent.

Cryptographic module of Subscribers: The CA does not hand over a signature creation device to the Subscribers. The signature creation devices of Subscribers must at least comply with the following certifications:

- EAL 4+ as regards the Common Criteria of ISO/CEI 15408 (compliant with Protection Profile CWA 14169 or certified as compliant with the Protection Profile of a Secure Signature Creation Device (SSCD) by a European governmental entity);
- FIPS 140-2 level 3

- QSCD or QSealCD within the meaning of regulation eIDAS (EU) No 910/2014.
- or equivalent.

For Certificates issued in accordance with OID 1.3.6.1.4.1.15819.5.1.3.6, the device must be a QSCD.

For Certificates issued in accordance with OID 1.3.6.1.4.1.15819.5.1.3.7, the device must be a QSealCD.

6.3 Other aspects of key pair management

6.3.1 Public key archival

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

6.3.2 Certificate operational periods and key pair usage periods

The maximum service life of the Certificates is:

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

6.4 Activation data

6.4.1 Activation data generation and installation

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

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

6.4.2 Activation data protection

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

6.4.3 Other aspects of activation data

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

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

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

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

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

Identification and authentication

The systems, applications and databases identify and authenticate users uniquely. All interactions between the system and a user are only possible after a successful identification and authentication. For every interaction, the system may check the identity of the interacting user. The authentication information is stored such that it is only accessible to authorised users.

Access control

The access rights and profiles to the equipment of the CA are defined and documented They also include the procedures for registering and deregistering users. The systems, applications and databases are defined in such a way as to differentiate between and administer the access rights of every user, at the user level, at the level of a membership in a user group or at both levels. It is thus possible to:

- complete refuse access to an object for users or user groups;
- limit the access of a user to an object to only operations that do not modify this object;
- grant access rights to an object by descending till the granularity level of the individual user.

No unauthorised user may grant or withdraw access rights to an object. Similarly, only authorised users may create new users, or delete or suspend existing users.

Administration and operation

The user of utility programs is restricted and controlled on infrastructure of the CA. The standard operating procedures for administration and operation of the CA are documented, monitored and updated regularly. The commissioning conditions (initial security configuration of the servers) are documented. The end of life conditions (destruction and scrapping) of the equipment are documented in order to guarantee the non-disclosure of sensitive information that said equipment might contain.

The sensitive hardware of the CA are covered by a maintenance procedure in order to guarantee the availability of the functions and information. The associated procedures are documented.

The staff concerned by these procedures are appointed by the management of the CA. Control measures for the maintenance actions have been applied.

Integrity of the components

The components of the local network are maintained in a physically secure environment. Periodic verifications of compliance of their configuration are carried out. Vulnerability patches are applied, after qualification, within a reasonable period after they are published.

Security of flows

Security measures are implemented in order to guarantee the source authentica-

tion, integrity, confidentiality and, if applicable, the data exchanged between the different components.

Logging and audit
The activity can be monitored via the event logs. It particularly helps in informing the persons concerned when a security incident is detected.

Supervision and control
Continuous surveillance is implemented and alarm systems are installed to detect, record and enable rapid reaction against any unauthorised and/or irregular attempt to access the (physical and/or software) resources.

Awareness raising
The CA implements appropriate awareness raising procedures for the staff.

6.5.2 Computer security rating

Not applicable.

6.6 Life cycle technical controls

6.6.1 System development controls

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

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

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

6.6.2 Security management controls

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

6.6.3 Life cycle security controls

Not applicable.

6.7 Network security controls

The services of the CA are installed on a network that is protected by firewall-type gateways that protect the networks based on their sensitivity. These gateways are configured to exclusively accept flows that are strictly necessary. Network flows are made redundant to ensure the availability of services. Moreover, the critical components are placed in zones with the highest security.

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

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

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

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

6.8 Time-stamping

All servers of the CA are synchronised with the same time source (UTC). The synchronisation of the servers is regularly checked.

7 Certificate, CRL and OCSP profiles

7.1 Certificate profiles

All Certificates issued by the CA are compliant with standards X.509, [ETSI 319 412-2], [ETSI 319 412-3] et [ETSI 319 412-5].

7.1.1 CA Certificates

Base fields

Field	Value
Version	v3
Serial number	defined by the tool
Signature	RSA/SHA-256
Issuer DN	C=FR, O=Cryptolog International, OU=0002 43912916400026, CN=Universign Primary CA Hardware
Validity	10 years
Subject DN	C=FR, O=Cryptolog International, OU=0002 43912916400026, CN=Universign CA Hardware
Public key	RSA 2048 bits

Certificate extensions

Field	OID	Crit.	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
CRL Distribution Points	2.5.29.31	No	
fullName			http://crl.universign.eu/universign_primary_ca_hardware.crl[3]
reasons			Absent
cRLIssuer			Absent
Certificate Policies	2.5.29.32	No	
policyIdentifier			2.5.29.32.0
policyQualifierId			1.3.6.1.5.5.7.2.1
qualifier			http://docs.universign.eu

[3]This URL is given for information purposes only and may change. Only the URL given in the certificate is valid.

7.1.2 Subscriber 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 CA Hardware
Validité	5 years
Subject DN	Name of the Subscriber, as defined in section 3.1.1
Public key	RSA 2048 bits

Certificate extensions

Field	OID	Crit.	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			True
keyEncipherment			False
dataEncipherment			False
keyAgreement			False
keyCertSign			False
cRLSign			False
encipherOnly			False
decipherOnly			False
Basic Constraint	2.5.29.19	No	
CA			False
CRL Distribution Points	2.5.29.31	No	
fullName			http://crl.universign.eu/universign_ca_hardware.crl[4]
reasons			Absent
cRLIssuer			Absent
Authority Info Access	1.3.6.1.5.5.7.1.1	No	
id-ad-ocsp	1.3.6.1.5.5.7.48.1		http://scah.ocsp.universign.eu/[5]
id-ad-caIssuers	1.3.6.1.5.5.7.48.2		http://www.universign.eu/cacert/universign_ca.cer[6]
Certificate Policies	2.5.29.32	No	
policyIdentifier			1.3.6.1.4.1.15819.5.1.3.(1/3/4/5/6/7)[7]
policyQualifierId			1.3.6.1.5.5.7.2.1
qualifier			http://docs.universign.eu
QC Statements[8]	1.3.6.1.5.5.7.1.3	No	
Qualified Certificate	0.4.0.1862.1.1		
QSCD[9]	0.4.0.1862.1.4		
Certificate's type	0.4.0.1862.1.6		0.4.0.1862.1.6.(1/2)[10]

[4]This URL is given for information purposes only and may change. Only the URL given in the certificate is valid.

7.2 CRL Profile

Base fields

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

CRL extensions

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

7.3 OCSP Profile

The CA offers to verify the status of Certificates issued by the OCSP (Online Certificate Status Protocol) responders. An OCSP responder helps to respond to requests for the status of a particular Certificate without needing to download the CRL. The OCSP of the CA complies with standard RFC 6960.

OCSP extensions The OCSP responses contain validity dates that allow the Relying Parties to determine whether the OCSP response is recent enough for the desired use. The CA responder does not use a nonce in these responses. Hence, the Relying Parties should not expect to receive a nonce in these responses if their request contained one.

[5]This URL is given for information purposes only and may change. Only the URL given in the certificate is valid.

[6]This URL is given for information purposes only and may change. Only the URL given in the certificate is valid.

[7]One of the value depend on the family of the Certificate.

[8]Present only for qualified Certificates.

[9]Present only if the private key corresponding to the Certificate if in a QSCD.

[10]0.4.0.1862.1.6.1 for natural person Certificates, 0.4.0.1862.1.6.2 for legal person Certificates.

8 Compliance audit and other assessments

8.1 Frequency or circumstances of assessment

Audits are conducted by the CA:

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

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

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

8.2 Identity/qualifications of assessor

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

8.3 Assessor's relationship to assessed entity

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

8.4 Topics covered by assessment

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

- the CP;
- the CPS;

- the components of the CA.

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

8.5 Actions taken as a result of deficiency

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

"Failed" verdict: The audit team issues recommendations to the CA. The CA can choose the measures to be applied.

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

"Successful" verdict: the CA confirms that the controlled component is compliant with the commitments of the CP and its announced practices.

8.6 Communication of results

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

9 Other business and legal matters

9.1 Fees

The pricing conditions of the currently applicable services are published on the website www.universign.com or are determined with the user of the service in a commercial contract.

9.1.1 Certificate access fees

Not applicable.

9.1.2 Revocation or status information access fees

Access to the CRL publishing service, OCSP responders and the revocation service is free of charge.

9.1.3 Fees for other services

No specific commitment.

9.1.4 Refund policy

The CA services are not subject to any reimbursement.

9.2 Financial responsibility

9.2.1 Insurance coverage

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

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

9.2.2 Other assets

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

9.2.3 Insurance or warranty coverage for end-entities

If damage is suffered by a Subscriber or a Relying Party of the service due to a breach of obligations by the CA, the CA may be required to compensate for the damages within the limits defined by its contractual commitments.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

The following information is considered to be confidential:

- the private keys of the CA,
- the activation data associated with the private keys of the CA,
- the event logs,
- the supporting documents of the registration files,
- the audit reports,
- the causes of revocation of Certificates,
- the business continuity, recovery and stoppage plans.

Other information may be considered as confidential by the CA.

The CA guarantees that only the staff members who need to know the confidential information have access to and may use said information. These staff members are bound by a confidentiality obligation.

9.3.2 Information not within the scope of confidential information

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

9.3.3 Responsibility to protect confidential information

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

The CA implements security procedures to guarantee the confidentiality of confidential information within the meaning of article 9.3.1. The CA complies with the laws and regulations in force in the territory of France as regards the provision of information to third parties in the context of legal or administrative proceedings.

9.4 Privacy of personal information

9.4.1 Privacy policy

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

The CA particularly pledges to comply with the regulations in force in the territory of France.

In particular, the CA informs the data subjects about their rights to access and correct erroneous data related to them, and in the cases and within the limits defined by the regulation, to oppose or delete some of their data, to limit its use or to request for its portability for the purpose of transmitting said data to a third party.

9.4.2 Personal information

Personal data contained in the registration files and not published in the Certificates or CRLs is considered to be confidential.

The processing of personal data is governed by the Personal Data Protection Policy.

9.4.3 Non-personal information

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

9.4.4 Responsibility to protect personal

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

9.4.5 Notice and consent to use personal information

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

The CA informs them about the rights that they are entitled to and the ways in which to avail of them through a Personal Data Protection Policy, which they expressly consent to.

9.4.6 Disclosure pursuant to judicial or administrative process

Personal information may be provided to legal or administrative authorities under the conditions defined by the regulations.

9.4.7 Other information disclosure circumstances

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

9.5 Intellectual property rights

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

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

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

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

9.6 Representations and warranties

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

- to protect and guarantee the integrity and confidentiality of their private cryptographic keys;
- to use their private cryptographic keys only pursuant to the conditions of and with the tools specified in the CP;
- to apply and comply with the requirements of the CP and the CPS applicable to them;
- to submit to the compliance audits conducted by the audit team mandated by UTN;

- to accept the consequences of these audits and in particular, to remedy any non-compliances that may be reported;
- to document their internal operating processes;
- to implement the (technical and human) resources needed for executing the operations that they are in charge of, while guaranteeing the quality and security of these operations.

9.6.1 Certification Authority

The CA is responsible for:

- the compliance of the CPS vis-à-vis the CP;
- the compliance of the Certificates with the CP;
- the compliance of all different components of the CA and the related controls with the principles of security.

The CA is responsible for damage caused to the Relying Parties if:

- the information contained in the Certificate does not correspond to the information contained in the registration file;
- the CA has not revoked a Certificate and/or has not published this information pursuant to the conditions defined in the CP.

9.6.2 RA service

See above.

9.6.3 Subscriber

The Subscriber:

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

9.6.4 Relying Parties

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

9.6.5 Other participants

No specific commitment.

9.7 Disclaimers of warranties

The limits of guarantee of the CA are defined in Subscriber Agreement and the Relying Party Agreement.

The CA does not have any power to represent or commit the UTN, or behave in any manner that is likely to create legal obligations, both expressly and tacitly in the name of the UTN.

9.8 Limitations of liability

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

The CA cannot be held liable for indirect damages resulting from the use of a Certificate.

The CA is not responsible for the use of the private keys associated with the Certificates or the activation data of these keys.

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

The CA cannot be held liable for any damages resulting from errors or inaccuracies in the information contained in the Certificates, when these errors or inaccuracies result directly from the erroneous nature of the information communicated by the Subscriber.

The liability of the CA is limited in accordance with the terms and conditions of the Subscriber Agreement and Relying Party Agreement or any other particular agreement signed between the CA and the user of the service.

9.9 Indemnities

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

9.10 Term and termination

9.10.1 Term

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

9.10.2 Termination

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

9.10.3 Effect of termination and survival

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

9.11 Individual notices and communications with participants

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

9.12 Amendments

9.12.1 Procedure for amendment

The CA may amend the CPS. These amendments take the form of new versions of the CPS. They are published on the publishing website of the CA or the UTN.

9.12.2 Notification mechanism and period

The CA informs the UTN about its intent to modify the CPS, by specifying the suggested modifications and the commenting period. If the CA administers its own publishing website, it must publish the change proposals on it. These change proposals are also published on the website of the UTN.

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

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

9.12.3 Circumstances under which OID must be changed

If there is a substantial change in the CPS, the Approval Board of the CA may decide that a change in OID is necessary.

9.13 Dispute resolution provisions

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

The maximum duration of the dispute settlement procedure is 3 months.

Alternative methods of amicable settlement of disputes are brought to the knowledge of users of the service via the Relying Parties or the Subscriber Agreement or any other contractual document.

9.14 Governing law

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

9.15 Compliance with applicable law

The provisions of the CPS are compliant with French law.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

No specific commitment.

9.16.2 Assignment

No specific commitment.

9.16.3 Severability

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

9.16.4 Enforcement (attorneys' fees and waiver of rights)

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

9.16.5 Force majeure

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

Force majeure covers the events that are normally qualified as such by French law and case-law.

9.17 Other provisions

9.17.1 Organization reliability

To guarantee the impartiality of its services, the CA ensures that the persons occupying Trusted Roles do not suffer from any conflicts of interest that would harm the impartiality of their tasks, especially when the said task consists of generating and revoking Certificates.

The CA pledges to carry out the tasks assigned to it by this CPS in complete independence and impartiality. It guarantees that the persons in charge of issuing and revoking Certificates shall act exclusively on their own instruction, free from any conflict of interest and in accordance with the CP.

It verifies the regularity of the Certificate issue and revocation applications with respect to the commitments defined in the CP.

The CA particularly pledges process issue and revocation requests only after ensuring that the procedures defined in the CP have been followed and that they can be executed smoothly.

The CA implements all legal means in its possession to ensure the honesty of persons occupying a Trusted Role. This verification is based on the inspection of the person's history, in which it is verified that this person has not been legally sentenced to a punishment that contradicts his duties. These verifications are carried out before assigning a person to a Trusted Role and are reviewed regularly (at least once every 3 years).

9.17.2 Accessibility

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

References

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

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

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

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

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

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

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

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

[**CNIL**]
Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)