CERTIFICATION PRACTICE STATEMENT

ANDORRAN PUBLIC ADMINISTRATION PKI

Govern d'Andorra

Version 3.0

Language: **English**

1. INTRODUCTION

1.1. Overview

The Andorran Public Administration's Public Key Infrastructure (PKI) has been created to ensure reliable, secure identity authentication while facilitating the confidentiality and integrity of electronic transactions in the Sistemas Informáticos Abiertos, SA (SIA) dependencies.. This document identifies the practices and procedures followed by the Office for Electronic Trust Services of the Principality of Andorra – hereinafter OSCEPA – ans SIA's ones when issuing digital certificates within this infrastructure.

This Certification Practice Statement is structured in accordance with document RFC-3647 "Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework", and is also in line with Law 35/2014, of 27 November , of electronic trust services of electronic trust services, article 10 of Law 9/2021, of 29 April, amending Law 35/2014, of 27 November, of electronic trust services of services of electronic trust, or marked by the eIDAS Regulation and in accordance with national law.

To make the document uniform and to make it easier to read and analyze, all the sections set out in RFC-3647 are included. When there is nothing planned in any section, the word "Does not apply" will appear.

1.2. Document name and identification

This document is the OSCEPA's Certification Practice Statement.

All certificates issued by the OSCEPA will contain a policy identifier corresponding to the applicable type of certificate.

The OSCEPA issues the following types of certificate, which may be identified through the certificate policy object identifier contained in the certificate's *certificatePolicy* extension. The types of certificate issued by the OSCEPA are identified below.

- Public corporate certificates, acquired by public sector organisations to fulfil their security needs.
- Citizenship certificates, issued by the Andorran Public Administration Certification Entity, or by other certification service providers when they have been authorised by the Public Administration.

Alongside, it issues the following types of certificate:

- Individual natural person certificates.
- Individual natural person under 16 to 18 years
- Individual natural person with regulated profession certificates.
- Corporate natural person at the service of a public administration certificates.
- Corporate natural person at the service of a private organisation certificates.
- Certificate for a representative of a private or public legal person or an entity without legal personality.
- Public law entity, body or public administration stamp.
- Company stamp.

1.3. PKI participants

The entities and people involved are:

- SIA as the entity that owns the infrastructure for the custody and issuance of root certificates and the typologies defined in article 1.2 of the CA Certification Entity of the Andorran Public Administration,
- OSCEPA as the entity responsible for the management of the Certification Body (Authority) of the Andorran Public Administration;
- Registration authorities;
- The signatories / holders;
- Subscribers;
- Third parties accepting the certificates issued.

1.3.1. Certification Authorities

SIA acts as the issuing company and custodian of the root certificates of the Root Authority. It owns the infrastructure that issues the certificates and is linked to the certification authority under the Government of Andorra for a service contract.

This is the component of the PKI responsible for issuing and managing digital certificates. It acts as a trusted third party between the Signatory (the Subscriber) and the Relying Party in electronic relations, linking a certain public key to a person.

A Certification Authority (CA) uses a Registration Authority (RA) to check and store documentation linked to the contents of the digital certificate.

The CA belongs to a legal entity indicated in the organisation field (O) of the associated digital certificate.

Information relating to the CA managed by the Andorran Public Administration can be found in this document or on the following website: https://www.signaturaelectronica.ad/jerarquia-politiques-i-practiques-de-certificacio

1.3.2. Registration Authorities

An RA may be a natural or legal person acting in accordance with this CPS and, if applicable, through an agreement signed with a specific CA, carrying out application management and certificate applicant identification and registration duties, as well as activities provided for in specific Certification Policies. RAs are authorities to which the CA delegates these tasks, the latter being ultimately responsible for the service.

For the purposes of this CPS, the following may act as an RA:

- The Certification Authority itself.
- Any national or international agent that maintains a contractual relationship with the CA and that goes through the registration and audit procedures that demonstrate that it fulfils the requirements set out in this document.

1.3.3. Applicant

The applicant is the person requesting the issuance of a certificate in their own name or on behalf of an organization.

1.3.4. Signatory

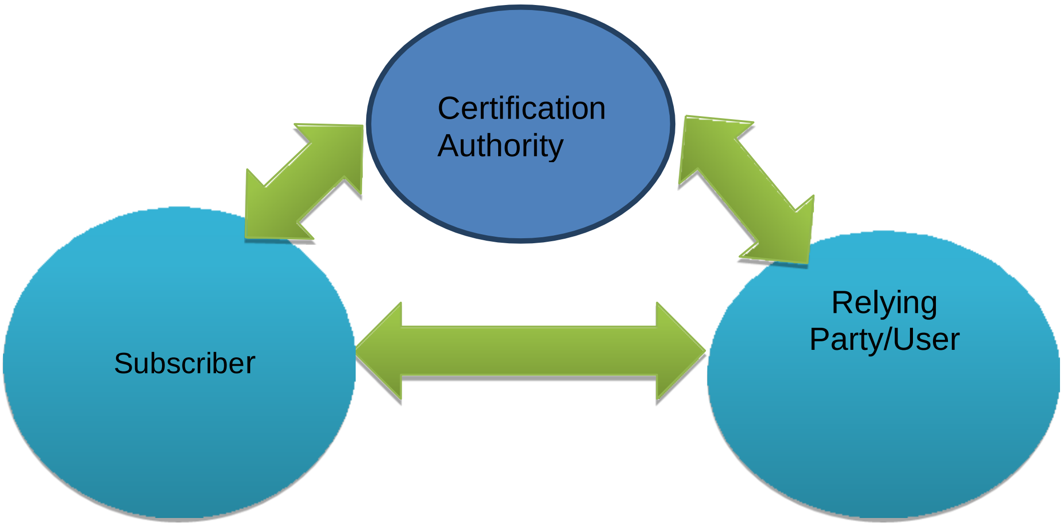
1.3.5. Signatory means the person or holder of the certificate who makes or creates the electronic signature.

1.3.6. Subscriber

In the event of a link between the signatory and an entity through an employment or contractual relationship, the subscriber is the entity that signs a contract with OSCEPA for the issuance of certificates to its users or third parties with a link to the company. However, you can request the revocation of the certificate when the signer's link with the subscriber ceases.

1.3.7. Relying Party

In this CPS, a Relying Party or User is considered the person who receives an electronic transaction carried out with a certificate issued by the CA and managed by the OSCEPA, and who voluntarily relies on this certificate.



1.3.8. Other participants

Does not apply.

1.4. Scope of application and uses

1.4.1. Appropriate uses of certificates

A certificate issued by OSCEPA may only be used for the purposes explicitly permitted and indicated in this CPS and the corresponding Certification Policy (PC), so there are certain limitations in the use of SIA certificates.

Certificates should only be used in accordance with the legislation applicable to them, especially taking into account the restrictions on imports and exports of cryptographic material that exist at any given time.

1.4.2. Forbidden uses of certificates

The certificates must be used for their own function and established purpose, without being able to be used in other functions and for purposes other than those described for each of them in section 1.4.1 Appropriate / permitted uses of certificates.

1.5. Policy Authority

This CPS defines the way in which the Certification Authority responds to all the security levels and requirements imposed by the corresponding Certification Policies.

The Certification Authority's activity may be subject to inspection by the Policy Authority (PA) or by personnel assigned by the PA.

For the hierarchies described in this document, the Policy Authority corresponds to the technical management of the OSCEPA.

1.5.1. Organisation administering the document

The working and control of this CPS is managed by OSCEPA management.

1.5.2. Organisation contact details

Address:	Carrer de la Grau, Edifici Prat del Rull, Andorra la Vella
Telephone:	+376 875700
Email:	oficina.certificacio@govern.ad

To report any security incidents relating to certificates, you may contact the Andorran Public Administration in writing at the email address oficina.certificacio@govern.ad

1.5.3. Person determining CPS's suitability for the policy

The management area of the OSCEPA therefore serves as the Policy Authority for the aforementioned Certification Authorities and Hierarchies and is responsible for the administration of the CPS.

1.5.4. Document management procedures

The publication of revised versions of this CPS must be approved by OSCEPA technical management.

The Andorran Public Administration publishes every new version on its website. The CPS is published in PDF format signed electronically with a digital certificate.

1.6. Acronyms and definitions.

1.6.1. Acronyms

CA	Certification Authority
RA	Registration Authority
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DES	Data Encryption Standard
DN	Distinguished Name
DSA	Digital Signature Algorithm
SSCD	Secure Signature Creation Device
SSCDSD	Secure Signature Creation Data Storage Device
FIPS	Federal Information Processing Standard Publication

IETF Internet Engineering Task Force

ISO International Organisation for Standardisation.

ITU International Telecommunications Union

LDAP Lightweight Directory Access Protocol

OCSP Online Certificate Status Protocol

OID Object Identifier

PA Policy Authority

CP Certification Policy

PIN Personal Identification Number

PKI Public Key Infrastructure

RSA Rivest-Shamir-Adleman. Type of encryption algorithm

SHA Secure Hash Algorithm

SSL Secure Sockets Layer Protocol designed by Netscape that has become a network standard. Allows for transmission of encrypted information between an internet browser and a server.

TCP/IP Transmission Control Protocol/Internet Protocol. Protocol system, defined in the IEFT. The TCP is used to divide information into packets at the origin before bringing it back together at the destination. The IP protocol directs the information to its recipient.

1.6.2. Definitions

Certification Authority This is the entity responsible for issuing and managing digital certificates. It acts as a trusted third party between the Subject/Signatory and the User, linking a certain public key to a person.

Policy Authority The person or persons responsible for all the decisions relating to the creation, administration, maintenance and elimination of certification policies and CPSs.

Registration Authority The entity responsible for managing applications and identifying and registering those who request a certificate.

Cross certification The establishment of trust between two CAs, through the exchange of certificates between the two by virtue of similar security levels.

Certificate A file that associates the public key with some data identifying the Subject/Signatory that is signed by the CA.

Public key A publicly known mathematical value used to verify a digital signature or for data encryption. Also known as signature verification data.

Private key A mathematical value known only by the Subject/Signatory and used to create a digital signature or for data decryption. Also known as signature creation data. The CA's private key will be used to sign certificates and CRLs.

CPS Set of practices adopted by a Certification Authority for issuing certificates in accordance with a specific certification policy.

CRL A file containing a list of the certificates that have been revoked in a certain period of time, signed by the CA.

Activation data Private data, like a PIN or password, used toactivate the private key.

SSCDSD Secure Signature Creation Data Storage Device. Software or hardware element used to store the Subject's/Signatory's private key so that only they have control over it.

SSCD Secure Signature Creation Device. Software or hardware element used by the Subject/Signatory to generate electronic signatures, so that cryptographic operations can take place within the device, controlled exclusively by the Subject/Signatory.

Entity Within the context of these certification policies, this is a company or organisation of any kind with which the applicant has some sort of link.

Digital signature The result of the transformation of a message, or any type of data, through the application of the private key along with some known algorithms, thus guaranteeing:

a) that the data has not been modified (integrity)
b) that the person signing the data is who they say they are (identification)
c) that the person signing the data cannot deny having done so (non-repudiation of origin)

OID Unique numerical identifier registered under ISO standardisation that refers to a certain object or object class.

Key pair The public key and the private key, which are linked mathematically.

PKI Set of hardware elements, software, human resources, procedures, etc. that make up a system based on the creation and management of public-key certificates.

Certification policy Set of rules that define the applicability of a certificate in a community and/or for a certain application, with common security and usage requirements.

Applicant Within the context of this certification policy, the applicant is a natural person with special powers to carry out certain procedures in the name and on behalf of the entity.

Subject/Signatory Within the context of this Certification Practice Statement, this is the natural person whose public key is certified by the CA and who has a private key valid for generating digital signatures.

User Within the context of this certification policy, this is the person who voluntarily puts their trust in the digital certificate and uses it as a way of checking the authenticity and integrity of the signed document

2. RESPONSIBILITY FOR PUBLICATION AND REPOSITORIES

2.1. Repositories

The OSCEPA has made its CA certificate public, which proves the validity of the digital certificates it issues and its CPS.

The repository can be found at https://www.signaturaelectronica.ad/ajuda

Consultation services are designed to guarantee availability 24 hours a day, 7 days a week.

The OSCEPA will request the holder's authorisation in advance before publishing the certificate.

2.2. Publication of certification information

The content of this CPS, together with the PCs for each type of certificate, will be available in the form of free access to the addresses indicated in section: 2.1 Repositories.

New versions of the document will be published to the web address provided, replacing the previous version. Previous versions of all documentation will be kept published.

2.3. Frequency of publication

The CPS and PCs will be published at the time of approval and will be republished at the time any changes to it are approved. Modifications will be made public on the website indicated in section 2.1 Repositories. The CA will add the revoked certificates to the relevant CRL within the time period stipulated in section 4.9.7 Frequency of issuance of CRLs..

2.4. Repository access control

The OSCEPA CA has controls in place to maintain the integrity of its internal repository, so that:

- The authenticity of the certificates can be verified.
- Unauthorized persons may not alter the data.
- Certificates will only be accessible in the cases or persons indicated by the signatory.
- Any technical changes that affect security requirements are detected..

3. IDENTIFICATION AND AUTHENTICATION OF CERTIFICATE HOLDERS

3.1. Naming

3.1.1. Types of name

The Signatory/Subscriber is described on certificates through a "Distinguished Name" (DN, Subject) in accordance with the X.501 standard. Descriptions in the DN field are reflected on every certificate profile page. It also includes a "Common Name" (CN) component.

Profile pages may be requested through customer support at oficina.certificacio@govern.ad or at https://www.signaturaelectronica.ad/ajuda.

For certificates corresponding to natural persons, the Signatory's identifier is made up of their full name plus their NIA (administrative ID number).

For certificates corresponding to legal persons, this identifier is composed of the organisation's name and its NRT (tax register number).

3.1.2. Meaning of names

All Distinguished Names must have a meaning, and the identification of the attributes associated with the Subscriber must be in a format that is legible for humans. See 7.1.4

3.1.3. Anonymity or Subscriber pseudonyms

Does not apply.

3.1.4. Rules used to interpret different name formats

The rules used by OSCEPA to interpret the distinctive names of the certificate holders it issues are ISO / IEC 9595 (x.500) Distinguished Name (DN) and ISO / IEC 9594-8 (X.509).

Certificates issued by OSCEPA comply with the recommendations of RFC 5280 ("Internet X.509 Public Key Infrastructure. Certificate and CRL Profile") regarding the use of the encoding of the attributes of the Issuer and Subject fields. . Specifically, through UTF8String encoding.

The RA has the association between these names or pseudonyms and the entities to which they are assigned.

3.1.5. Uniqueness of names

Within the same CA, the same Subscriber name cannot be assigned twice. A unique name is achieved by adding the unique tax identifier to the name that distinguishes the certificate holder.

3.1.5.1. Issuance of various natural person certificates for one holder

In this CPS, the Subscriber may request more than one certificate as long as the combination of the following values in the application is different to those of a valid certificate:

- Natural person's administrative ID number (NIA)
- Company's tax register number (NRT)
- Type of certificate (certificate description field)

As an exception, this CPS allows a certificate to be issued when the NIA, NRT and type coincide with a valid certificate, as long as there is a distinguishing element between the two in the TITLE and/or DEPARTMENT fields.

3.1.6. Procedure for resolving name disputes

Any dispute concerning the ownership of names shall be resolved in accordance with the provisions of Section 9.13 Claims and Jurisdiction of this CPS.

OSCEPA reserves the right to reject an application for a certificate due to a name conflict

3.1.7. Recognition, authentication and function of trademarks and other distinctive

Oscepa does not make any commitments regarding the use of trademarks in the certificates or determine whether the signatory is entitled to the trademark. We also reserve the right to reject an application for a certificate due to a trademark dispute.

3.2. Initial identity validation

3.2.1. Methods to prove possession of private key

Because the key pair generation procedure depends on the type of certificate issued, proof of ownership of the private key will be described in each specific certification policy.

The private key for both Root AC and Subordinate ACs is securely generated in a cryptographic hardware module (HSM) and will never be released.

3.2.2. Entity identification

Identity authentication for client certificates is specified in the corresponding Certification Policy.

3.2.3. Identification of an individual's identity

Identity authentication for client certificates is specified in the corresponding Certification Policy.

3.2.4. Non-verified Subscriber information

These certification practices do not permit the inclusion of non-verified Subscriber information in the "subject" of a certificate.

3.2.5. Verification of the powers of representation

Each Certification Policy will establish the procedure for verifying the powers claimed for each case

3.2.6. Organization and domain or IP authentication

Does not apply

3.3. Identification and authentication of re-key requests

3.3.1. Validation for routine certificate re-key

Re-key requests are identified through the certificate to be re-keyed. The certificate will not be re-keyed if 5 years have passed since its last physical verification or equivalent process.

3.3.2. Identification and authentication of a re-key request following a revocation

The identification and authentication policy for a certificate re-key after a revocation is the same as the policy for initial registration.

3.4. Identification and authentication of revocation request

The process for making a revocation request is established in section 4.9.3 of this document.

The OSCEPA may, on its own initiative, request the revocation of a certificate if it discovers or suspects that the Subscriber's private key has been compromised, or if it discovers or suspects any other event that requires this measure to be taken.

4. OPERATIONAL REQUIREMENTS FOR CERTIFICATE LIFE CYCLE

To manage the certificate life cycle, the OSCEPA uses a platform that deals with certificate applications and the registration, publication and revocation of all certificates issued.

4.1. Certificate application

4.1.1. Who can request a certificate?

This section depends on the type of certificate and is included in its corresponding Certification Policy. The PC also sets out the steps to be followed in processing them.

4.1.2. Requests Registration

The OSCEPA or an intermediary of the OSCEPA that acts as RA to manage the application for the certificate, is responsible for the registration procedure. This information will be donated to the data base of the registration authority for such subsequent consultations, on the status of the sol·licitud of the sol·licitant or of the sol·licitats certificates per a particular subscriber.

4.2. Certificate application processing

At the moment in which the OSCEPA or an intermediary of the OSCEPA that acts as an RA represents a request for a certificate, the registration process will be carried out with the corresponding registration application associated with the Certification Authority.

During the application process, there is a verification that the user really pertany to the system, this verification is due to term mitjançant consultation to the OSCEPA repository, in order to obtain the information of the sol·licitant necessarily.

4.2.1. Execution of identification and authentication functions

It is the responsibility of the RA to reliably carry out the identification and authentication of the sol·licitant. This process has to be done prior to the issuance of the certificate.

This section is dependent on the type of certificate in particular and is linked to the corresponding Certification Policy.

4.2.2. Approval or rejection of requests:

At the time of the appearance or equivalent procedure, the RA verifies the information provided by the applicant, including the validation of the identity of the signer or subscriber. If this information is correct, it is appropriate to sign the binding legal instrument between the signer and OSCEPA.

Please consult the specifics of each type of certificate in the specific Policy for each certificate.

Then you can proceed to the issuance of the certificate.

4.2.3. Time to process application

Does not apply.

4.3. Certificate issuance

4.3.1. CA actions during the issuing process

This information is specified in the relevant Certification Policy..

4.3.2. Notification of issuance to the Subscriber

This information is specified in the relevant Certification Policy.

4.4. Acceptance of certificates

4.4.1. Conduct that constitutes acceptance of the certificate

Acceptance of the certificate is the action by which the holder initiates obligations with respect to the trusted service provider SIA. The certificate will be accepted at the time the binding legal instrument between the applicant and the SIA has been signed and the certificate is in the possession of the signatory.

As proof of acceptance there must be an acceptance form signed by the signatory. You will be able to start using the certificate from the date the acceptance form was signed.

In the field of the centralized signature certificate, in the case of generation of the electronic signature certificate, the same act of issuance entails the implicit acceptance of the signature certificate and the acceptance and signature of the document in accordance with the issuance of the qualified certificate of centralized signature.

From the moment of acceptance, this CPS in relation to the signatory deploys all its effects.

4.4.2. Publication of the certificate by the CA.

Certificates will be published in the repositories for this purpose.

4.4.3. Notification of the issuance of a certificate by the CA to other entities

Does not apply.

4.5. Use of key pair and certificates

4.5.1. Subscriber's use of certificate and private key

The responsibilities and limitations of use of the key pair and the certificate will be established in the corresponding PC. The holder will only be able to use the key pair and the certificate after accepting the conditions of use, established in the CPS and PC, the document of acceptance means and in accordance with what is established in the extensions "Key Usage" and "Extended KeyUsage" certificate.

The application of these limits will largely depend on the correct implementation by third-party computer applications, and the regulation will fall outside the scope of this document.

After the certificate expires or the certificate is revoked, the holder must stop using the associated private key and the corresponding certificates.

CA	Key Usage	Extended key usage	Basic Constraint
Andorran Public Administration Certification Entity	critical, cRLSign, keyCertSign	–	**critical,CA:true**
natural person on dscf	critical, nonRepudiation	clientAuth, emailProtection	**critical,CA:false**
Natural person Minor and between 16-18 certificates on DSCF -	critical, nonRepudiation	clientAuth, emailProtection	**critical,CA:false**
Natural person with regulated profession on dscf	critical, nonRepudiation	clientAuth, emailProtection	**critical,CA:false**
Natural person with regulated profession on dscf – encrypted	critical, keyEncipherment, dataEncipherm	clientAuth, emailProtection	**critical,CA:false**
natural person at the service of an organisation on dscf	critical, nonRepudiation	clientAuth, emailProtection	**critical,CA:false**
natural person at the service of the administration on dscf	critical, nonRepudiation	clientAuth, emailProtection	**critical,CA:false**
natural person at the service of the administration on dscf – encrypted	critical, keyEncipherment, dataEncipherm	clientAuth, emailProtection	**critical,CA:false**
company stamp (legal person) on dscf– electronic stamp	critical, nonRepudiation	clientAuth, emailProtection	**critical,CA:false**

CA	Key Usage	Extended key usage	Basic Constraint
company stamp (legal person) on software	critical, digitalSignature , keyEncipherme	clientAuth, emailProtection	**critical,CA:false**
public law entity, body or public administration stamp on dscf	critical, nonRepudiation	clientAuth, emailProtection	**critical,CA:false**
public law entity, body or public administration stamp on SOFTWARE	critical, digitalSignature , keyEncipherment,	clientAuth, emailProtection	**critical,CA:false**
representative of legal person on dscf	**critical, nonRepudiation**	**clientAuth, emailProtection**	**critical,CA:false**

4.5.2. Relying Party's use of public key and certificate

Third parties relying on the certificates may use the certificates for the purposes set out in this CPS and the corresponding PC, and in accordance with the "Key Usage" and "Extended Key Usage" fields of the certificate.

It is the responsibility of third parties to verify the status of the certificate using the services offered by SIA specifically for this purpose and specified in this document.

4.6. Renewal of certificate

4.6.1. Circumstances for certificate renewal

In the area of the AC of Oscepa, the renewal of certificates will not be carried out without a change of keys.

4.7. Certificate re-key

The particular conditions of renewal are specified in the corresponding Certification Policy.

4.8. Modification of certificates

To modify a certificate, a new application is required. The old certificate will be revoked and a new one will be issued with the correct information.

In the case of a certificate substitution process, this will be considered a renewal and will therefore count in the calculation of the period of renewal without physical presence, as set out by the law.

A modification can take place as a renewal when the Subscriber's or the key holder's attributes that make up the uniqueness control provided for in this policy have not changed.

If the modification application is made within the standard period established for certificate renewals, this renewal will be granted.

4.8.1. Circumstances for certificate modification

Does not apply.

4.8.2. Who can request a certificate modification?

Does not apply.

4.8.3. Processing certificate modification requests

Does not apply.

4.8.4. New certificate issuance notification to the Subscriber

Does not apply.

4.8.5. Conduct that constitutes acceptance of the modified certificate

Does not apply.

4.8.6. Publication of modified certificate by the CA

Does not apply.

4.8.7. Certificate issuing notification from CA to other entities

Does not apply.

4.9. Suspension of certificates

Does not aply

4.10. Revocation/suspension of certificates

Revocation of a certificate is invalid and irreversible.

Revocations take effect from the moment the indication of said revocation is included in the consultation service on the validity of OSCEPA certificates.

All certificate revocation status query services must have the information available consistently at the time a certificate is revoked or suspended. Given the nature of each service, CRLs and OCSPs, there is the possibility of a small out of sync that in no case will exceed five (5) minutes. This should be taken into account by third parties who need to carry out validations of the revocation status of certificates issued by this PSC with the maximum guarantees on the synchronization of revocation information.

4.10.1. Reasons for revocation

As a general rule, a certificate may be revoked for the following reasons:

- Modification of any of the details contained in the certificate.
- Incorrect or incomplete information in the certificate application, or any alteration or modification to the circumstances verified for the certificate to be issued.
- No payment received for the certificate.

Circumstances that affect the security of the key or the certificate.

- Compromised private key or breach of the issuing Certification Entity’s infrastructure or systems, if this affects the reliability of any certificates issued from the time of the incident onwards.
- The Certification Entity’s failure to comply with the requirements established for certificate management procedures, provided for in this CPS.
- Compromise or suspected compromise of the security of the key, of the Signatory’s certificate or of the certificate holder.
- Unauthorised third-party use of or access to the Signatory’s or the certificate holder’s private key.
- Any irregular use of the certificate by the Signatory or the certificate holder, or any lack of diligence in the protection of the private key.

Circumstances that affect the security of the cryptographic device.

- Compromise or suspected compromise of the cryptographic device’s security.
- Loss or destruction caused by damage to the cryptographic device.
- Unauthorised third-party access to the Signatory’s or the certificate holder’s activation data.

Circumstances affecting the Signatory or their representative.

- End of the relationship between the Certification Entity and the Signatory or their representative.
- Modification or termination of the underlying legal relationship or cause that led to the issuance of the certificate to the Signatory or their representative.
- The applicant’s breach of the pre-established requirements for applying for a certificate.
- The Signatory’s or their representative’s breach of their obligations, responsibility and guarantees established in the corresponding legal instrument or in this Certification Practice Statement.
- The unexpected incapacity or death of the Signatory or their representative.
- The termination of the legal person Signatory, of the purpose for which authorisation was granted by the Signatory to their representative, or of the relationship between the Signatory and their representative.
- The Signatory’s request to revoke the certificate, in accordance with the provisions of this CPS.
- A firm decision issued by the competent administrative or legal authority.

Other circumstances

- The issuance of a certificate that does not fulfil the requirements established in this Certification Practice Statement.
- The termination of the Certification Entity's service, in accordance with the provisions of the corresponding section of this CPS.

To prove the alleged need for revocation, the corresponding documents must be submitted to the RA or CA, according to the cause of the request.

- If the revocation is requested by the certificate holder or the natural person who applied for a legal person certificate, they must sign and submit a declaration indicating the certificate to be revoked and the reason behind the request, as well as proving their identity to the RA.
- If the revocation is requested by a third party, they must submit an authorisation from the natural person certificate holder or from the legal representative of the legal person certificate holder that indicates the reasons behind the revocation request, as well as proving their identity to the RA.
- If the revocation is requested by the entity linked to the certificate holder due to the termination of their relationship, they must provide proof of this situation (revocation of powers, termination of contract, etc.) and prove their identity to the RA as an authorised representative of the entity.

Signatories have revocation codes they can use when revoking online or via a telephone call to support services.

4.10.2. Who can request a revocation?

A certificate revocation may be requested by

- The Subject/Signatory
- The applicant
- The entity (through a representative)
- The RA or CA
- Furthermore, third parties or concerned parties may communicate any fraud, misuse, inappropriate conduct or incorrect data, in which case the RA or CA may revoke the certificate after checking the validity of these causes for revocation.

4.10.3. Revocation request procedure

All requests must be made:

- Through the ONLINE Revocation Service, via access to the revocation service located on the OSCEPA website, by entering the Revocation PIN.

https://www.signaturaelectronica.ad

- Through a visit to the RA in its public opening hours and presentation of the Signatory/Subscriber's or applicant's ID document. The Signatory/Subscriber must fill up the certificate/s revocation request.
- By sending the OSCEPA a document signed by a representative for the entity with sufficient powers of representation requesting the revocation of the certificate.
- Through the Siacert centralized certificate management portal platform.

The OSCEPA website contains all the information regarding certificate revocation processes.

4.10.4. Grace period for revocation request

The revocation period begins immediately or in 24 hours lap of time when the OSCEPA or an RA has authenticated evidence of the revocation of a certificate. This revocation is then incorporated into the next CRL to be issued and in the management platform database that runs the OCSP responder.

4.10.5. Deadline for CA to process the revocation request

The OSCEPA will process a revocation request immediately starting from the procedure described in point 4.10.3,

In the case of a revocation caused by a mistake in the issuance of the certificate, the holder will be notified in advance to agree on the time in which it will be substituted.

In any event, and following these certification practices, the OSCEPA can revoke a certificate unilaterally and immediately for security reasons, without the holder being able to claim any kind of compensation.

4.10.6. Revocation check requirements for Relying Parties

Before using a certificate, the Relying Party must check its status and consult the last CRL issued, which can be downloaded at the URL that appears in the certificate's CRL Distribution Point extension.

The OSCEPA always issues CRLs signed by the CA that issued the certificate. The CRL contains a field (*NextUpdate*) with the date of its next update.

4.10.7. Frequency with which CRLs are issued

CRLs for end-of-entity certificates will be generated every 24 hours or more, if any, at the time a certificate is revoked with a 24-hour validity.

The CRL of CA Certificates (ARLs) is issued every 12 months or when a revocation occurs.

If the latest CRL is issued for the validation of end-entity certificates, the nextUpdate field will be set to "99991231235959Z", as established by the ETSI EN 319 411-1 standard.

4.10.8. Maximum latency for CRLs

OSCEPA will immediately publish the CRL that has been generated in any of the cases indicated in section 4.9.7, through an automated process..

4.10.9. Availability of online revocation check

Certificate status information will be available online 24 hours a day, 7 days a week.

In the event of a system failure, or any other factor beyond the control of the CA, the CA will make every effort to ensure that this information service is not unavailable for longer than the maximum 24-hour period.

This term does not apply in cases where OSCEPA is not responsible for including power supplies, communications, hardware and software components of which OSCEPA is not the owner or the like.

4.10.10. Requirements for online revocation check

OSCEPA has planned a certificate validation service through the OCSP protocol. This service will be open access and should consider:

- Check the address contained in the Certificate Information Access (AIA) extension of the certificate.
- Check that the OCSP response is signed. The OCSP response signing certificate issued by AC OSCEPA complies with the standard: RFC 6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".
- The information provided through the OCSP service is updated at least every four days and the response is valid for 10 days.

4.10.11. Other available ways to find out revocation information

To use the free access CRL service, consider:

- In any case, the last CRL issued must be checked, which can be downloaded from the URL contained in the final entity certificates themselves in the "CRL Distribution Point" extension or in the same CPS as the corresponding ones. PC.
- The user will need to additionally check the pending CRLs in the certification chain of the hierarchy.
- The user must ensure that the revocation list is signed by the authority that issued the certificate they want to validate.
- Expired certificates that are expired will not be removed from the CRL, maintaining them for fifteen (15) years for qualified certificates and at least 7 years for the rest.

4.10.12. Special requirements for revocation due to compromised keys

Does not aplly

4.10.13. Circumstances for suspension

Does not aplly

4.10.14. Who can request a suspension?

Does not aplly

4.10.15. Suspension request procedure

Does not aplly

4.10.16. Suspension period limits

Does not apply.

4.11. Certificate status checking services

4.11.1. Operational characteristics

The OSCEPA offers an issued certificate and revocation list consultation service. These services are available publicly on its website: https://www.signaturaelectronica.ad

4.11.2. Service availability

Consultation services are designed to guarantee availability 24 hours a day, 7 days a week.

4.11.3. Optional characteristics

Does not apply.

4.12. End of subscription

Once the certificate's validity period has ended, subscription to the service will be terminated. As an exception, the Subscriber may keep the service active by requesting renewal of the certificate, with as much notice as required by this Certification Practice Statement.

4.13. Key escrow and recovery

4.13.1. Key escrow and recovery policy and practices

The root key of the root CA as well as those of the SIA Subordinate CAs have been generated on cryptographic security modules, complying with necessary security levels.

The particular conditions of custody of the private keys issued to users are specified in the corresponding Certification Policy. Otherwise, the TSP will never guard or copy the private key issued to users. Therefore, the TSP will never be able to recover the user key. If it is lost, the certificate must be revoked and a new one issued.

4.13.2. Session key encapsulation and recovery policy and practices

Does not apply.

5. PHYSICAL, MANAGEMENT AND OPERATIONAL CONTROLS

5.1. Physical security controls

The aspects related to physical security controls are set out in detail in the documentation that SIA has developed for this purpose. This section should include the most relevant measures taken.

5.1.1. Location and construction

The buildings where the SIA CA infrastructure is located have access control security measures, so that only duly authorized persons are allowed to enter, who meet the following physical requirements:

- Located in specific locations to prevent damage from possible fires.
- Absence of windows outside the building. Surveillance cameras in restricted access areas.
- Card and password based access controls.
- Fire protection and prevention systems.
- Protection of wiring against damage and interception of data transmission.

5.1.2. Physical access

Physical access to SIA premises where certification processes are conducted is limited and protected through a combination of physical and procedural measures.

It is limited to expressly authorized personnel, with identification at the time of access and registration of the same, including closed circuit television filming and its archive.

The facilities have presence detectors at all vulnerable points as well as alarm systems for intrusion detection with warning through alternative channels.

Access to the rooms is with ID card and fingerprint readers, managed by a computer system that maintains an automatic check-in and check-out.

5.1.3. Electricity supply and air conditioning

SIA AC computer equipment is properly protected against power outages or power outages, which could damage or disrupt service.

The facilities have a current stabilization system, as well as its own generation system with sufficient autonomy to maintain this supply for the time required for the orderly and complete closure of all systems.

The computer equipment is located in an environment where air conditioning (temperature and humidity) is guaranteed to be suitable for optimal working conditions.

Periodic checks of generators and power sources are performed to validate proper operation

5.1.4. Exposure to water

The SIA facilities where the equipment is located are protected to prevent exposure to water, through moisture detectors and other safety mechanisms.

Periodic checks of these elements are made.

5.1.5. Fire prevention and protection

The facilities where the SIA AC equipment is located have the appropriate fire protection measures, such as smoke detectors, ion sensors, alarms, fire extinguishers and HFC-227 gas in case of fire.

Periodic checks are made of all these items.

5.1.6. Storage system

SIA has established the necessary procedures to have backups of all the information of its productive infrastructure. Backups are stored securely.

SIA has prepared backup plans for all sensitive information and that considered necessary for the persistence of its activity.

5.1.7. Waste disposal

A waste management policy has been adopted that guarantees the destruction of any material that may contain information as well as a management policy for removable media.

5.1.8. Off-site backup

SIA has backups in different locations that meet the precise security measures and with adequate physical separation.

5.2. *Procedural controls*

For security reasons, information on procedural controls is considered confidential and only part of it is included. SIA also guarantees that its systems are operated and managed securely, and for this purpose establishes and implements procedures for the functions that affect the provision of its services.

5.2.1. Trusted roles

Trusted roles guarantee the separation of roles, which improves control and limits internal fraud by not allowing one person to control all certification functions from start to finish and granting minimum privileges, where possible.

To determine the sensitivity of the role, the following elements are taken into account:

- Duties associated with role.
- Access clearance.
- Monitoring of the role.
- Training and awareness.
- Skills required.

Internal auditor:

Responsible for carrying out operational procedures. This person is external to the Information Systems department.

Internal auditor tasks cannot be carried out simultaneously to Certification tasks and Systems tasks. These roles are subordinate and report to the operations division and technical management.

System administrator:

Responsible for the correct operation of the hardware and software used for the certification platform.

System administrator tasks are incompatible with certification tasks and operations auditors' tasks.

CA administrator:

Responsible for action to be carried out with cryptographic material or via any function that involves the activation of Certification Authorities' private keys described in this document, or any of their elements.

CA administrator tasks are incompatible with certification and systems tasks.

CA operator:

Along with the CA administrator, responsible for keeping the activation material for the cryptographic keys. Also responsible for backup and maintenance operations at the CA.

CA operator tasks are incompatible with those of the CA administrator. The CA operator cannot carry out auditor or internal auditor tasks either.

RA operator:

Responsible for approving certification applications made by the Signatory.

RA operator operations are incompatible with those of the RA administrator. The RA operator cannot carry out internal or external auditor tasks either.

Revocation operator:

Revocation operator tasks are incompatible with audit tasks.

Security officer:

Responsible for controlling, monitoring and ensuring compliance with the security measures defined by the OSCEPA's security policies. Must deal with all logical, physical, network-related and organisational aspects of information security.

5.2.2. Number of people required per task

The AC SIA guarantees at least three people to perform the tasks that require a multi-person control detailed below:

- Generation of the key of the ACs.

- Recovery and backup of the private key of the ACs
- Issuance of CA certificates.
- Activation of the private key of the ACs.
- Any other activity performed on the hardware and software resources that support the root CA..

5.2.3. Identification and authentication for each role

The people assigned for each role are identified to ensure that each of them carries out the operations assigned to them.

Access to resources is based on roles, ensuring access to them through secure devices..

5.2.4. Roles that require separation of duties

CWA 14167-1 establishes the following incompatibilities between roles:

- Incompatibility between security officer and HSM operator.
- Incompatibility between administrative roles (system administrator and RA operator).
- Incompatibility between HSM administrators and operators.
- Incompatibility between the system auditor role and any other role

5.3. Personnel controls

5.3.1. Qualifications, experience and clearance requirements

The staff who provide their services in the field of the SIA Certification Authority have sufficient knowledge, experience and training for the correct assignment of the assigned functions. For this reason, SIA carries out the personnel selection processes it deems necessary in order for the employee's professional profile to be as close as possible to the characteristics of the tasks to be performed.

OSCEPA personnel are qualified and have been properly instructed to perform the operations assigned to them.

Personnel in trusted roles are not affected by personal interests that conflict with the carrying out of their assigned role.

The OSCEPA guarantees that the registration personnel or RA administrators are trustworthy and belong to an organisation to which registration tasks have been delegated.

The RA administrator must have completed a preparation course for carrying out request validation tasks.

In general, the OSCEPA will dismiss an employee from their trusted role if it discovers that they have carried out a criminal act that may affect their ability to carry out their duties.

The OSCEPA shall not assign a trusted or management role to anyone not suitable for the position, especially if they have been found guilty of a crime or offence that affects their suitability for the position. For this reason, investigations allowed by the applicable legislation will be made in relation to the following aspects:

- Studies, including qualifications.
- Previous jobs (in the past five years), including professional references and verification that the candidate really did these jobs.
- Arrears

5.3.2. Background check procedures

Personnel selection processes are those already defined by SIA. These internships ensure the required experience, qualification, and history requirements for each position, whether in a trusted role or not.

Within its human resources procedures, before hiring anyone, the OSCEPA carries out the relevant investigations. Within the Government of Andorra, the procedures set out in Law 1/2019 of 17 January on public service are followed.

In the application for the vacancy in certain roles, the OSCEPA notifies the candidate that they must be willing to undergo prior investigations and that, if they refuse, their application will be rejected. Furthermore, the concerned party must provide their unequivocal consent to being investigated and to the processing and protection of their personal data, in accordance with personal data protection legislation.

5.3.3. Training requirements

SIA and OSCEPA provide the staff related to the operation of the CA with all the necessary information and documentation on the operational procedures related to it.

SIA and OSCEPA monitor the training and the level of confidence of the staff and carry out the necessary tests to be able to assess the appropriate level of assimilated knowledge..

5.3.4. Retraining requirements and frequency

The OSCEPA carries out the retraining courses needed to ensure certification tasks are carried out correctly, especially when substantial changes are made to them.

5.3.5. Frequency and sequence of task rotation

Does not aplly

5.3.6. Sanctions for unauthorised actions

The OSCEPA through the Civil Servant Secretariat has an internal system of sanctions, described in its human resources policy, to be applied when an employee carries out unauthorised actions, which may lead to their dismissal.

5.3.7. Personnel hiring requirements

The employees hired to carry out trusted tasks must first sign the confidentiality clauses and operational requirements implemented by the Andorran Government. Any action that compromises the security of the accepted processes may, once evaluated, lead to the termination of the employment contract.

Should all or part of the certification services be carried out by a third party, the checks and precautions established in this section, or elsewhere in the CPS, will be applied to and fulfilled by the third party carrying out the certification service operation tasks. In any case, the Certification Entity will be responsible for the correct provision of the services.

5.3.8. Documentation provided to personnel

The OSCEPA provides all personnel with documentation detailing assigned functions, especially security regulations and the CPS.

These documents are found in an internal repository accessible by any OSCEPA employee. The repository contains a list of documents with which employees must be familiar and comply.

The documentation personnel require at any given time to properly fulfil their duties will also be provided.

5.4. Event recording procedures

5.4.1. Types of event recorded

SIA will record all events related to the operation and management of the system, as well as those related to its security, a

mong others:

- Starting and stopping applications.
- Successful or failed login and logout attempts.
- Successful or failed attempts to create, modify, or delete authorized system users.
- Those related to the management of the life cycle of certificates and CRLs.
- Complete reports of attempts at physical intrusion into the infrastructures that support the issuance and management of certificates.
- Backup, archive and restore. Changes in system configuration.
- Software and hardware updates.
- System maintenance.
- Staff changes.
- Changes to the keys of the Certification Authority.
- Changes to certificate issuance policies and this CPS.
- Records of destruction of material containing key information, activation data or personal information of the subscriber.
- Reports of commitments and discrepancies.
- Physical access records.
- Cryptographic module lifecycle events, such as receiving, using, and uninstalling this key generation

ceremony and key management databases.

Operations are divided into events, so information about one or more events is saved for each relevant operation. Registered events have at least the following information:

- Category: Indicates the importance of the event.
    - Informational: Events in this category contain information about successful operations.
    - Mark: Each time an administration session starts and ends, an event of this category is logged.
    - Warning: Indicates that an unusual event was detected during an operation, but did not cause the operation to fail.
    - Error: Indicates the failure of an operation due to a predictable error.
    - Fatal Error: Indicates that an exceptional circumstance has occurred during an operation.
- **Date**: Date and time the event occurred.
- **Author**: Distinctive name of the authority generating the event.
- **Role**: Type of Authority generated by the event.
- **Event Type**: Identifies the type of event, distinguishing, among other things, cryptographic events from user interface, library.
- **Module**: Identifies the module that generated the event. The possible modules are:
    - AC
    - RA
    - Information repository.
    - Information storage control libraries.

Description: Textual representation of the event. For some events, the description is followed by a list of parameters whose values will vary depending on the data on which the operation was run. Some examples of the parameters that are included for the description of the "Certificate Generated" event are: the serial number, the distinguished name of the certificate holder issued, and the certification template that was applied..

5.4.2. Frequency with which audit logs are processed

Logs will be analyzed manually when necessary, for example in the event of a system alert triggered by the existence of an incident, and there will be no set frequency for this process..

5.4.3. Retention period for audit logs

SIA keeps online the information regarding qualified certificates generated by audit records until it is filed. Once filed, the audit records will be kept for at least fifteen (15) years and the one for the remaining certificates for at least 7 years.

5.4.4. Protection of audit logs

Sia protects audit log files from readings, modifications, deletions, or other unauthorized manipulation by using logical and physical access controls.

AC software logs are protected by cryptographic techniques, so no one except the event viewing application, with proper access control, can access them.

5.4.5. Audit log backup procedures

SIA makes regular backups of audit records generated by the CA.

The OSCEPA, through the Department of Information Systems, has established a suitable backup procedure so that, should the relevant files be lost or destroyed, the corresponding backup copies of the audit logs will quickly be available.

The OSCEPA has implemented a secure audit log backup procedure; every week, a backup is made of all the audit logs on an external medium.

A copy is also kept at an off-site storage centre.

5.4.6. Audit information collection system

Event audit information is collected internally and automatically by the operating system, the network and the certificate management system, as well as by manually generated data, which is stored by the duly authorised personnel. All of this makes up the audit log accumulation system.

5.4.7. Notification to event-causing subject

The action of the audit log files is not expected to be automatically notified to the cause of the event.

5.4.8. Vulnerability analysis

SIA, in accordance with the internal procedure in its security policy, periodically reviews discrepancies in log information and suspicious activities..

5.5. *Record archival*

SIA, in accordance with the internal procedure in its security policy, periodically reviews discrepancies in log information and suspicious activities.

5.5.1. Type of records archived

The types of events that are logged in the file are:

- Certificates and revocation lists.
- Data related to the certificate application and registration process.
- Certification Practices and Policies and their history.
- Audit logs of section 5.4.1. Type of event.
- Error events in the processes performed..

5.5.2. Archive retention period

SIA will retain all information and documentation relating to qualified certificates for a minimum of fifteen (15) years and that relating to other certificates for at least 7 years.

For audit records, the provisions of section 5.4.3 are provided, always taking into account any particularities specified in the Certificate Certification Policy corresponding to the data involved..

5.5.3. Archive protection

The log files are protected by encryption, so that no one except the display applications themselves, with their access control, can access them.

The destruction of a log file can only be done with the permission of the system administrator, security coordinator, and SIA audit administrator. Such destruction may be initiated by the written recommendation of any of these three authorities or of the audited service administrator, and provided that the minimum retention period of fifteen (15) years has elapsed. Such destruction will require express written authorization..

5.5.4. Archive backup procedures

The backup files will be backed up according to the standard measures established by SIA for the backups of the other information systems. This backup runs automatically in the Backup Center.

The OSCEPA has an off-site storage centre to guarantee the availability of the copies of the electronic file archive. Physical documents are stored in secure places that can only be accessed by authorised personnel.

The OSCEPA carries out an incremental backup of all its electronic documents at least once a day and a complete backup for data recovery needs at least once a week.

5.5.5. Requirements for record time-stamping

The information systems used by SIA guarantee the recording of the time in which they are carried out. The time instant of the systems comes from a secure source that states the date and time. All the servers that make up the Electronic Certification Infrastructure are synchronized in date and time. The time sources used, based on the Network Time Protocol (NTP), are synchronized using the Royal Institute and Navy Observatory as a reference.

Server synchronization is performed at least once every 24 hours..

5.5.6. Audit information collection system

The information collection system is internal to the Authority and corresponds to SIA..

5.5.7. Procedures for obtaining and verifying archived information

SIA-registered events are protected by cryptographic techniques so that no one but their own event viewing and management applications can access them. Only authorized personnel have access to physical media files and computer files, to perform integrity or other checks.

This verification must be performed by the audit administrator who must have access to the PKI event log integrity verification and control tools.

The OSCEPA has a computer security document that describes the process for verifying that archived information is correct and accessible.

5.6. Key changeover

The procedures for providing, in the event of a key change, a new CA public key to certificate holders and third party acceptors are the same as for providing the existing public key. Consequently, the new key will be published in the SIA repository (see section 2.1 Repositories)..

5.7. Recovery in event of compromised key or disaster

5.7.1. Compromised key or incident management procedures

SIA has established a Contingency Plan that defines the actions to be taken, the resources to be used and the personnel to be used in the event of an intentional or accidental event that disables or degrades the resources and services provided.

The Contingency Plan includes, among other aspects, the following:

- The redundancy of the most critical components.
- The response from an alternative backup center.
- Complete and periodic review of backup services.

In the event that the security of the signature creation data of any Certification Authority is affected, SIA will inform all certificate holders, supervisory bodies and known third party acceptors that all certificates and revocation lists signed with this data are no longer they are valid. The service will be restored as soon as possible..

5.7.2. Corruption of resources, applications or data

In the event of a hardware, software, and / or data resource failure event, SIA will shut down CA services until the security of the environment can be verified, if necessary by replacing the affected components with others. whose integrity is duly verified. At the same time, an audit will be carried out to identify the cause of the alteration and to ensure that it is not reproduced.

In the event that the certificates issued are affected, the users will be notified of the fact and a new certification will be carried out..

5.7.3. Entity's private key compromised

SIA considers the commitment or suspected compromise of the AC private key to be a disaster. In the event that the security of the CA's private key is compromised, SIA will carry out the following actions:

- Revoke the certificate of the current CA, so that the certificates issued by this CA are no longer valid.
- Inform all certificate holders and subscribers that all certificates issued by this CA are no longer valid. It shall also notify the supervisory body of this fact.
- Revoke the certificate of the subordinate CA and all the certificates in force and issued by this CA. If the revoked certificate is the root CA, you will remove the certificate from the repository and notify the trusted service provider's website.
- Publish the corresponding ARL.
- Generate a new CA with a new signing key and certificates.
- Restore service as soon as possible.
- Inform the state security forces and / or the Attorney General's Office and / or the Judicial Authority in case there may be criminal activities..

5.7.4. Business continuity following a disaster

SIA will re-establish critical services (revocation and publication of revoked certificates) in accordance with this CPS within 24 hours following a disaster or unforeseen emergency based on the existing contingency and business continuity plan.

SIA has an alternative center, if necessary, for the implementation of certification systems..

5.8. Termination of CA or RA

5.8.1. Certification Authority

Prior to the cessation of its activity, Oscepa will carry out the following actions:

- It will provide the necessary funds (through a civil liability insurance) to continue the completion of the revocation activities.

- It will inform of the termination of all the signatories / subscribers, the third party that it trusts and other ACs with which it has agreements or another type of relation, with a minimum anticipation of six months.
- It will revoke any authorization to subcontracted entities to act on behalf of the CA in the procedure for issuing certificates.
- It will transfer its obligations regarding the maintenance of log and log information for the period of time indicated to subscribers and users.
- The private keys of the CA will be destroyed or deactivated for use.

Oscepa will keep the certificates active and the verification and revocation system until all certificates issued have expired.

5.8.2. Registration Authority

When the RA ceases to perform its functions, it will transfer the records it maintains to OSCEPA, as long as there is an obligation to keep the information archived, and if this is not the case, it will be destroyed in a secure and credible manner. reliably..

6. TECHNICAL SECURITY CONTROLS

6.1. Key pair generation and installation

6.1.1. Key pair generation

Both the root CA and OSCEPA subordinate CA key pairs are generated and stored in a secure cryptographic hardware (HSM) module by SIA, which meets the necessary security requirements.

The keys and certificates of entities are issued in accordance with the provisions of the Certification Policy corresponding to the type of certificate.

6.1.2. Delivery of private key to Subscriber

The private key will be sent to the holder in accordance with the provisions of the Certification Policy for each type of certificate.

6.1.3. Delivery of public key to certificate issuer

The public key will be sent to the holder in accordance with the provisions of the Certification Policy for each type of certificate..

6.1.4. Delivery of public key from CA to Relying Parties

Both the root CA and the subordinate CA certificate are published in the repositories indicated in section 2.1 Repositories of this same CPS

6.1.5. Size of keys

OSCEPA root AC keys are 4096 bits.

OSCEPA subordinate CA keys are 4096 bits.

The length of the certificate holders' keys is specified in the corresponding Certification Policy.

6.1.6. Public key generation parameters and quality assurance

The root CA and subordinate CA public key is encrypted according to RFC 5280 and PKCS # 1. The key generation algorithm is RSA.

The key generation parameters for each type of certificate issued are specified in the corresponding Certification policy.

The procedures and means of checking the quality of the parameters for each type of certificate issued are specified in the corresponding Certification Policy.

6.1.7. Purpose of the use of keys (field KeyUsage de X.509 v3)

Permitted uses of the key are defined in accordance with the Certification Policy for each type of certificate.

All certificates issued by OSCEPA contain the “Key Usage” extension defined by the X.509 v3 standard, which is rated as critical. Additional limitations may also be set by using the "Extended Key Usage" extension.

Please note that the effectiveness of limitations based on certificate extensions sometimes depends on the operation of computer applications that have not been created or controlled by OSCEPA..

6.2. Protection of private key and standards for cryptographic modules

6.2.1. Controls and standards for cryptographic modules

The modules used to create the root CA and SIA subordinate CA keys meet the required security requirements and guarantee their protection.

The implementation of each of the CAs, taking into account the use of cryptographic security modules (HSM), involves the following tasks:

- Initialization of the HSM.
- Creation of the means of access for the roles of administration and operator.
- Generation of AC keys.

The measures taken for the custody of the signatories' keys are detailed in their corresponding Certification Policy..

6.2.2. Multi-person control (n out of m) of private key

Access to the private key, both of the Root AC and of the Subordinate AC, requires the presence of a minimum of three people with specific roles to be able to access it, these roles being both physical and control logical.

6.2.3. Private key escrow

The private keys of both the root CA and the subordinate CA, are stored and protected in the HSM and never leave the same.

6.2.4. Private key backup

SIA backs up the CA's private key during the process of generating it.

These copies are made for business continuity purposes for disaster recovery. Backups have the same level of security as the original key, since it is part of the same cryptographic security module.

Copies of the key are saved in a different location than the one where the AC is located.

6.2.5. Private key archival

The particular conditions of custody of the private keys issued to users are specified in the corresponding Certification Policy. Otherwise, the private keys of the signers' qualified certificates will never be archived by the CA.

6.2.6. Transfer of the private key to or from the cryptographic module

Private key transfer can only be done between cryptographic modules (HSMs) and requires the intervention of three people with different roles.

6.2.7. Storing the private key in the cryptographic module

Private keys are generated in the cryptographic module at the time of activation of each of the ACs that make use of the modules..

6.2.8. Private key activation method

As stated in Section 6.2.2 Multi-Person Control of the Private Key, the private key of both the root CA and the subordinate CA is activated by initializing the CA software through the minimum character of three people with specific roles. This is the only way to activate this private key..

6.2.9. Private key deactivation method

An administrator can deactivate the CA key by stopping the CA software. For its reactivation, the minimum intervention of the roles described in the previous sections is required..

6.2.10. Private key destruction method

When necessary, SIA will destroy the CA's private key and its backup to ensure that no residual information that can be used to rebuild the private key is maintained.

In general terms, destruction should always be preceded by a revocation of the certificate associated with the key, if it is still valid.

6.2.11. Cryptographic module capabilities

The cryptographic devices used by the certification authorities meet the necessary security requirements to ensure the protection of the keys of the certification authorities.

These devices are resistant to intrusive tamper protection..

6.3. Other aspects of key pair management

6.3.1. Public key archival

SIA, in accordance with the provisions of article 26 of Andorran Law 35/2014, of 27 November, on electronic trust services, will retain all OSCEPA public keys for the period required by applicable law and in accordance with the provisions of this document..

6.3.2. Period of use for public and private keys

The certificate and key pair of the OSCEPA root generated by SIA generated by the SIA are valid for fifteen (15) years and those of the OSCEPA subordinate CA generated by SIA of fifteen (15) years.) years.

The expiration will automatically result in the invalidation of the certificates, causing the permanent cessation of its operation in accordance with its own uses and, consequently, the provision of trusted services. If there is no cessation of TSP activity, prior to the expiration of the CA certificate, a new CA (new key pair) will be generated under the same security conditions as the one about to expire. and all parties will be notified of the existence of the new CA. The certificate of the new CA will be published and distributed as specified for the current one in this CPS.

This whole process of generating the new CA will be done well in advance and with a view to minimizing the impact on third parties.

The period of validity of the other certificates will be established by the Certification Policy applicable to each one.

6.4. Activation data

6.4.1. Generation and activation of activation data

To enable SIA private keys, SIA requires minimal intervention from the system administrator, CA operators, and HSM administrators. This is the only way to activate this private key.

In the case of the keys of the final entity certificates, the generation of activation data is indicated in the corresponding certification policy..

6.4.2. Protection of activation data

Only authorized personnel are aware of the activation data of the private keys of the root CA and subordinate CA.

For final entity certificates, they will be detailed in their corresponding certification policy..

6.4.3. Other aspects of activation data

Does not apply.

6.5. Computer security controls

The data concerning this section is considered confidential information and is only provided to those who can prove the need to know it, as in the case of both external and internal audits and inspections. The OSCEPA uses reliable systems to offer its certification services The OSCEPA has carried out computer audits and checks to ensure that the management of its computer assets meets the required level of security for the management of electronic certification systems.

With regard to information security, the information management systems certification standard ISO 270001 is fulfilled.

The equipment used is initially configured with the appropriate security profiles by the OSCEPA's systems personnel in the following aspects:

- Operating system's security configuration.
- Applications' security configuration.
- Correct system sizing.
- Configuration of Users and permissions.
- Configuration of log events.
- Backup and recovery plan.
- Antivirus configuration
- Network traffic requirements

6.5.1. Specific computer security technical requirements

The data concerning this section is considered confidential information and will only be provided to those who prove the need to know it.

However, with regard to the management of information security, SIA follows the scheme provided for in UNE-ISO 27002 (formerly called ISO 17799), Code of Good Practice for Information Security..

6.5.2. Assessment of computer security

SIA continuously evaluates its security level in order to identify possible weaknesses and establish the corresponding corrective actions through external and internal audits, as well as the continuous performance of security controls.

Products used to provide certification services have Common Criteria and / or FIPS 140-2 certification..

6.6. Life cycle security controls

The data concerning this section is considered confidential information and is only provided to those who can prove the need to know it, as in the case of both external and internal audits and inspections..

6.6.1. System development controls

The security requirements are required, from the beginning, both in the acquisition of computer systems and in the development of the same as they could have some impact on the security of SIA.

6.6.2. Security management controls

SIA has a security organization in charge of its management on the basis of the UNE-ISO / IEC 27001: 2007 standard, which is subject to periodic audits by AENOR.

6.6.2.2. Security management

The Civil Servants Department carries out the activities required to train its employees in and raise their awareness of security issues. The materials used for training and the documents that describe the processes are updated after being approved by a security management group.

To achieve this, it uses an annual training plan.

Via a contract, the OSCEPA demands the security measures equivalent to those of any external provider involved in certification practices.

6.6.2.3. Classification and management of information and goods

The Information Systems Department keeps an inventory of assets and documentation and has implemented a procedure to manage these materials to guarantee their usability.

The Government's security policy details its information management procedures, where information is classified according to its level of confidentiality.

The documents are catalogued according to three levels: public,internal uses and confidential.

6.6.2.4. Management operations

The Information Systems Department has implemented an appropriate incident management and response procedure, through the implementation of a system of alerts and the generation of periodic reports. The OSCEPA’s security document contains the details of the incident management process.

The OSCEPA keeps records of the whole process relating to the duties and responsibilities of the personnel involved in the checking and handling of elements contained in the certification process.

Media processing and security

All media are processed securely, in accordance with the information’s classification requirements. Media that contain sensitive data are destroyed securely if they will no longer be required.

System planning

The Information Systems Department keeps a record of all equipment’s capacity. Alongside each system’s resource control application, a potential resizing may be considered.

Incident reports and responses

The Information Systems Department has implemented a procedure to track incidents and their resolution, through which responses and an economic assessment of the resolution of the incident are recorded.

Operational procedures and responsibilities

The OSCEPA defines the activities assigned to persons in trusted roles, who are different from persons assigned non-confidential, everyday operations.

6.6.2.5. Access system management

The OSCEPA will go to all reasonable efforts to confirm that the access system is limited to authorised persons.

In particular:

General CA

- There are controls based on firewalls, antivirus and high-availability IDS.
- Sensitive data is protected by cryptographic techniques or access controls with strong authentication.
- The OSCEPA has documented its user registration and termination procedure and detailed access policy in its security policy.
- The OSCEPA implements the procedures needed to guarantee that operations are carried out in accordance with the roles policy.
- Each person is associated with a role to carry out certification operations.
- The OSCEPA's personnel takes responsibility for their actions through the confidentiality commitment they sign with the company.

Certificate generation

Authentication for the issuance process is carried out via an m out of n operators system to activate the CA private key.

Revocation management

Revocation is carried out through strong authentication in the authorised administrator's applications. Log systems will generate the proof that guarantees the non-repudiation of the action taken by the CA administrator.

Revocation status

The revocation status application has access control that revolves around certificate-based authentication in order to avoid any attempts to modify revocation status information.

6.6.2.6. Management of cryptographic hardware life cycle

The OSCEPA makes sure that the cryptographic hardware used to sign certificates is not handled during transport by inspecting the delivered material.

The cryptographic hardware is moved via media prepared to avoid any handling.

The OSCEPA records all the relevant details of the device to add it to the assets catalogue.

At least two trusted employees are required to use the cryptographic certificate signature hardware.

The OSCEPA carries out tests periodically to make sure the device is working correctly.

The cryptographic hardware device is only handled by trusted personnel.

The CA signature private key stored on the hardware will be deleted once the device has been removed.

The configuration of the CA system, as well as any modifications and updates to it, are documented and monitored.

The OSCEPA holds a device maintenance contract. Changes or updates are authorised by the security officer and reflected in the corresponding work records. These configurations must be carried out by at least two trusted persons.

6.6.3. Life cycle security evaluation

SIA has defined security controls throughout the life cycle of the systems with possible impacts on the security of the same.

6.6.4. Lifecycle Controls for Secure Signature Creation Devices

SIA will perform the appropriate reviews to verify the validity status of the certification of secure signature creation devices.

The source of the query is: https://esignature.ec.europa.eu/efda/notification-tool/#/screen/browse/list/QSCD_SSCD

6.7. Network security controls

The OSCEPA protects physical access to network management devices and uses an architecture that sorts the generated traffic based on its security characteristics, thus creating clearly defined sections of network. This division is carried out using firewalls.

Any confidential information transferred over insecure networks is encrypted by SSL protocols.

The policy used to configure the systems and security elements is based on an initial state of total blockage, from which the services and ports needed to provide the services are gradually opened. Reviewing access is part of the tasks to be carried out in the systems department.

The administration systems and production systems are located in separate environments.

6.8. Time-stamping

System time is synchronized with the Royal Navy Observatory, following the NTP protocol over the Internet. The NTP protocol description can be found in RFC5905. Network Time Protocol Version 4: Protocol and Algorithms Specification.

Synchronization will be done at least every 24 hours..

7. CERTIFICATE, CRL AND OCSP PROFILES

7.1. Certificate profile

The certificates issued by the SIA systems will comply with the provisions of the following standards and technical specifications:

- ETSI EN 319 412-5: Profiles for Trust Service Providers issuing certificates; Part 5: Extension for Qualified Certificate profile.
- RFC 5280 “Internet X.509 Public Key Infrastructure. Certificate and CRL Profile ”.
- RFC 3739 “Internet x509 Public Key Infrastructure. Qualified Certificates Profile ”.
- Profiles of Certificates derived from Law 6/2020, of 11 November, regulating certain aspects of trusted electronic services, Law 40/2015 of 1 October, on the Legal Regime of the Public Sector (LRJ) and in Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS).
- ETSI EN 319 412-2 (Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons).
- ETSI EN 319 412-2 3 (Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons).
- ETSI EN 319 412-4: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificats.
- ETSI TS 119495: Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements a the payment services Directive (EU) 2015/2366.

7.1.1. Version number

OSCEPA issues X.509 Version 3 certificates.

7.1.2. Certificate extensions

User certificates issued by SIA on behalf of the OSCEPA link a person's identity to a specific public key. To guarantee the authenticity and non-repudiation, all this information will be electronically signed by OSCEPA, the entity in charge of the broadcast.

7.1.3. Algorithm object identifiers (OID)

Object Cryptographic Algorithm (OID) Identifier: SHA-256 with RSA Encryption (1.2.840.113549.1.1.11).

7.1.4. Name format

Certificates issued by SIA on behalf of OSCEPA contain the “distinguished name X.500” of the issuer and the certificate holder in the “issuer” and “subject” fields respectively

7.1.5. Name restrictions

The OSCEPA may impose name restrictions (using the certificate extension “name constraints”) in subordinate CA certificates issued to third parties so that only the set of certificates allowed on that extension may be issued by the subordinate CA.

7.1.6. Certification policy object identifier (OID)

The OID of this policy is 2.16.20.2.1.13.1.1.

All awarded certificates have a policy identifier starting from base 1.3.6.5.5.7.48. and Government of Andorra (OSCEPA) = 2.16.20.2.

7.1.7. Use of “Policy Constraints” extension

The OSCEPA may impose policy restrictions (using the certificate extension “policy constraints”) in subordinate CA certificates issued to third parties so that only the set of certificates allowed on that extension may be issued by the subordinate CA.

7.1.8. Policy qualifiers syntax and semantics

Does not aplly

7.1.9. Processing semantics for the critical “Certificate Policy” extension

The “Certificate Policy” extension identifies the policy that defines the practices the OSCEPA explicitly associates with the certificate. The extension may contain a policy qualifier. See 7.1.6.

7.2. CRL profile

7.2.1. Version number

The CRLs issued by the OSCEPA are X.509 version 2.

7.2.2. CRL and extensions

CRLs issued by SIA on behalf of OSCEPA will comply with RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile, April 2002..

7.3. OCSP profile

Certificates issued by AC SIA comply with RFC 6960 “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP”.

The information provided through the OCSP service is updated at least every four days.

7.3.1. Version number

OCSP Responder certificates will use the X.509 Version 3 (X.509 v3) standard.

7.3.2. OCSP extensions

The main extensions for OCSP are as shown in the following table:.

Field	Mandatori	Crítical
1. Issuer Alternative Name	No	No
2.Authority/Subject keyIdentifier	No	No
3. CRL Distribution Point	No	No
4. Key usage	Yes	Yes
5. Enhanced Key usage	Yes	No
7. NoCheck	No	No

8. COMPLIANCE AUDITS

8.1. Frequency or circumstances of audits

Periodic internal audits will be conducted, usually on an annual basis. OSCEPA will also carry out an external audit every year and be carried out by a recognized and accredited body in order to confirm that the certificate issuing services comply with the requirements established by law. This audit will take into account the audit carried out at SIA in the same year.

Extraordinary audits may be carried out in the event of possible security incidents and / or for any other reason approved by the Security Officer.

Finally, the qualified trust service provider will be audited, at least every 24 months, by a conformity assessment body as established in eIDAS, exactly with the Conformity Assessment Report under the regulation (EU) No. 910/2014, on electronic identification and trust services in electronic transactions in the internal market (eIDAS regulation)...

8.1.1. Audits at Registration Authorities

All RAs are audited. These audits are carried out discretionally at least every two years and are based on a risk analysis. Audits check that the requirements set out by this CPS are being fulfilled during the execution of the registration tasks detailed in the signed service contract.

In internal audits, samples of issued certificates are taken to check that they were processed correctly.

8.2. Identification and name of auditor

Audits can be both internal and external. In this second case, they are carried out by companies of recognized prestige in the field of audits. The auditor will have accredited qualifications and experience to perform these types of tasks

8.3. Relationship between auditor and CA

Apart from the audit function, the external auditor and the audited party (OSCEPA + SIA) must not have any relationship that could lead to a conflict of interest. In the case of internal auditors, they may not have a functional relationship with the area being audited. Auditors are independent of the audited activity and free from bias and conflict of interest. Auditors will maintain an objective attitude to the order of the audit process to ensure that the findings and conclusions of the audit will be based solely on the evidence of the audit.

The audit team is fully independent, having previously verified for these purposes:

- Lack of employment, business or empowerment ties with the audited organization.
- No direct or indirect interest with audited slowness.
- The absence of links of marriage, consanguinity or affinity up to the first degree or collateral consanguinity up to the second degree, with the employers, administrators or those responsible for the area of information systems and / or information security.
- Lack of familiarity or trust, due to influence and excessive proximity to the administrators or directors of the audited entity.
- The previous non-execution of services related to the definition and implementation of security measures in the audited organization by the audit team.
- The fees offered do not represent a significant percentage of the company's turnover..

8.4. Topics covered by audit

The audit will determine the adequacy of OSCEPA + SIA services with this CPS. It will also determine the risks of non-compliance with the operations defined in these documents.

In general, the criteria set out in section 3.3 (“Introduction to conformity assessment of Certification Authorities”) and 3.5 (“Guidance on the conformity assessment process”) of CWA 14172-2. And in particular for TSPs qualified in accordance with the eIDAS Regulation and according to the technical standards ETSI TS 319 401, ETSI TS 319 411-1 and ETSI TS 319 411-2 and ETSI TS 119 495 additionally for PSD2 certificates.

8.5. Action taken as a result of deficiencies

The identification of deficiencies detected as a result of the audit will lead to corrective action. The person responsible for approving the policies, in collaboration with the auditor, will be responsible for determining them with the utmost diligence..

8.6. Communication of results

The audit team will communicate the results of the audit to the OSCEPA CA Policy Approval Officer, the system security manager, as well as the CA administrators and administrators where the incidences..

9. LEGAL ASPECTS AND OTHER ISSUES

9.1. Fees

9.1.1. Certificate issuance and renewal fees

Prices for certification services or any other related service are available and updated on the Official Bulletin of the Principality of Andorra website https://www.bopa.ad.

A specific price is published for each type of certificate, except those that are subject to prior commercial negotiations.

9.1.2. Certificate access fees

Access to issued certificates is free. The OSCEPA implements controls to avoid any mass downloads of certificates. Any other circumstance that, according to the OSCEPA, must be considered in this regard will be published on the OSCEPA website https://www.signaturaelectronica.ad.

9.1.3. Fees for access to information on status of certificates or revoked certificates

Oscepa provides access to information on the status of certificates or certificates revoked free of charge, through an online OCSP service and the publication of the corresponding CRLs..

9.1.4. Fees for access to the contents of these Certification Practices.

Access to the content of this CPS is free and provided on the OSCEPA website: https://www.signaturaelectronica.ad/jerarquia-politiques-i-practiques-de-certificacio.

9.1.5. Refund policy

The OSCEPA does not have a specific refund policy; it invokes the general regulations in force.

9.2. Financial liability

9.2.1. Insurance cover

In its activity as a CSP, the OSCEPA has a civil liability insurance policy that covers its liabilities and compensates users of its services, the Subject/Signatory, the User and third parties for any damages for a total amount of 600,000 euros.

9.2.2. Other assets

Does not apply.

9.2.3. Insurance or guarantee for end entities

See section 9.2.1.

9.3. Confidentiality of business information

9.3.1. Type of information to be kept confidential

The OSCEPA will consider all information not expressly catalogued as public to be confidential. Information declared confidential will not be shared without express written consent from the entity or organisation that gave the information its confidential status, unless there is a legal obligation to do so.

The OSCEPA has an adequate data processing policy and confidentiality agreement templates to be signed by all those who have access to confidential information.

9.3.2. Type of information considered non-confidential

The OSCEPA considers the following information non-confidential:

- Certificates.
- The uses and financial limits outlined in the certificate.
- The period of validity of the certificate, as well as the date of issue of the certificate and the expiry date.
- The serial number of the certificate.
- The different states or situations of the certificate and the start date of each one, in particular:
    - or pending generation and / or delivery, valid, revoked or expired and the reason that caused the change of status.

- Certificate revocation lists, as well as other revocation status information

9.3.3. Duty to protect confidential information

The OSCEPA is responsible for protecting confidential information generated or communicated during all operations. The delegated parties, such as the entities that administer the subordinate issuing CAs or the Registration Authorities, are responsible for protecting confidential information generated or stored through their own means. For end entities, Subscribers of certificates are responsible for protecting their private key and all activation information (meaning passwords or PINs) needed to access or use the private key.

9.3.3.1. Disclosure of information regarding revocation of certificates

The OSCEPA discloses information regarding the revocation of certificates through the periodic publication of the corresponding CRLs.

The OSCEPA offers a CRL and Certificate consultation service on the following website: http://crl2.govern.ad/GovernAndorra_SUB01.crl

The OSCEPA offers an online status consultation service for certificates based on the OCSP standard on the following website: http://va.govern.ad. The OCSP service offers standardised responses under RFC 2560 regarding digital certificates' status: it indicates whether the consulted certificate is active or revoked and whether it has been issued or not by the Certification Authority.

9.3.3.2. Delivery to competent authority

The OSCEPA will provide information requested by the corresponding competent authority or regulatory body, in the cases and in the way established in the legislation in force.

9.4. Personal data protection

9.4.1. Personal data protection policy

The OSCEPA complies with the applicable data protection regulations in all cases and at all times. In particular, it has adapted its processes to the EU General Data Protection Regulation 2016/679 (GDPR).

9.4.2. Privacy Policy.

OSCEPA has a privacy policy that can be consulted at:

https://www.signaturaelectronica.ad/oscepa-privacitat.html.

9.4.3. Information not considered private

An individual's personal information available in the content of a certificate or CRL is not considered private, as it is required to provide the requested service, without prejudice to the rights granted to the holder of the personal data by virtue of GDPR legislation.

9.4.4. Duty to protect private information

The data controller is responsible for protecting private information adequately.

9.4.5. Notice and consent to use private information

Before embarking on a contractual relationship, the OSCEPA will offer the concerned parties information regarding the processing of their personal data and how to exercise their rights and, if applicable, will seek the required consent to process the data in a way other than the main purpose of providing the requested services.

9.4.6. Disclosure pursuant to judicial or administrative proceedings

Whether considered private or otherwise, personal data may only be disclosed if necessary for the formulation, exercising or defence of claims, whether through a judicial procedure or through an administrative or extrajudicial procedure.

9.4.7. Other information disclosure circumstances

Personal data will not be passed on to third parties, unless legally required.

9.5. Intellectual property rights

The OSCEPA holds the intellectual property rights to this CPS.

9.6. Obligations and civil liability

9.6.1. CA's obligations and liability

9.6.1.1. CA

In accordance with the provisions of this CPS and of the regulations in force regarding the provision of certification services, the OSCEPA is obligated:

- To respect the provisions set out in this CPS.
- To protect its private keys securely.
- To issue certificates in accordance with this CPS, with certification policies and with the applicable technical standards.
- To issue certificates in accordance with the information it holds, free of any data entry errors.
- To issue certificates that contain at least the information defined by the regulations in force for qualified or recognised certificates.
- To publish issued certificates in a directory, while respecting applicable data protection regulations in all cases.
- To suspend and revoke certificates in accordance with the provisions of this policy and publish these revocations in the CRL.
- To inform Subjects/Signatories of the revocation of their certificates, in the time and way established by the legislation in force.
- To publish this CPS and the corresponding certification policies on its website.
- To notify Subjects/Signatories and the related RAs of any modifications to this CPS and to the certification policies.
- Not to store or copy the Subject's/Signatory's signature creation data, except for encryption certificates and for cases in which this storage or copying is legally permitted or required.
- To protect signature creation data with due care while it is held by the OSCEPA, if applicable.
- To establish generation and storage mechanisms for information relevant within the activities described here and protect it from loss, destruction or forgery.
- To retain information regarding the issued certificate for the minimum period required by the regulations in force.

The OSCEPA will be liable for any damage caused to users by its services, whether this user is the Signatory/Subscriber or the Relying Party, and to other third parties under the terms established in the legislation in force and the certification policies.

In this regard, the OSCEPA is the only party liable (i) for the issuance of certificates, (ii) for the management of certificates throughout their life cycle, and (iii) in particular, if required, for the revocation of certificates. Specifically, the OSCEPA will fundamentally be liable for:

- The accuracy of all the information contained in the certificate on its date of issuance, through the confirmation of the applicant's details and the RA's practices.
- Guaranteeing that, when the certificate is delivered, the Signatory/Subscriber holds the private key that corresponds to the public key provided or identified in the certificate when the process calls for this, through the use of standardised requests in PKCS#10 format.
- Guaranteeing that the public and private keys work in a joint and complementary manner by using certified cryptographic mechanisms and devices.
- Correspondence between the requested certificate and the delivered certificate.
- Any other liability established by the legislation in force.

In compliance with the legislation in force, the OSCEPA has taken out a civil liability insurance policy, which covers the requirements set out by the certification policies affected by these certification practices.

9.6.2. RA's obligations and liability

RAs are entities to which the CA delegates registration and certificate application approval tasks. RAs are therefore also obligated to act in accordance with the terms defined in the Certification Practices for certificate issuance, and especially:

- To respect the provisions set out in this CPS.
- To protect the private keys to be used to carry out the RA's functions.
- To check the identity of the Subjects/Signatories and certificate applicants when necessary, certifying the Signatory's identity, in the case of individual certificates, or the key holder's identity, in the case of an organisation certificate, in accordance with the provisions of the corresponding sections of this document.
- To check the accuracy and authenticity of the information provided by the applicant.

- To provide the Signatory, in the case of an individual certificate, or the future key holder, in the case of an organisation certificate, with access to the certificate.
- To deliver the relevant cryptographic device, if applicable.
- To archive the documents provided by the applicant or the Signatory for the period established in the legislation in force.
- To respect the provisions of the contracts signed by the OSCEPA and the Subject/Signatory.
- To inform the OSCEPA of the causes for revocation, when they are aware of them.
- To offer basic information on the policy and on how to use the certificate, including information on the OSCEPA and the applicable Certification Practice Statement, and on obligations, powers and liabilities.
- To offer information on the certificate and the cryptographic device.
- To collect information and evidence from the holder when they receive the certificate and, if applicable, the cryptographic device, and to seek their acceptance of these elements.
- To inform the private key holder of the allocation method and of the details needed to activate the certificate and, if applicable, the cryptographic device, in accordance with the provisions of the corresponding sections of this document.

Information on the Subscriber's use of the certificate and their liabilities are provided through the acceptance of usage clauses before the certificate application can be made and via email.

RAs' liability

RAs enter into a service provision contract with the OSCEPA, through which the OSCEPA delegates registration tasks to the RA, which fundamentally consist of:

- 1.- Obligations before the certificate is issued.
    - Adequately informing applicants of their obligations and liabilities.
    - Adequately identifying applicants, who must be persons empowered or authorised to apply for a digital certificate.
    - Properly checking the validity of the applicant's details and those of the entity, if there is an affiliation- or representation-based relationship between them.
    - Accessing the Registration Authority Android application to manage applications and issued certificates.
- 2.- Obligations once the certificate is issued.
    - Entering into Digital Certification Service Provision contracts with applicants. In most issuance processes, this contract is formalised through the acceptance of the terms and conditions on the website pages that are part of the certificate issuance process. The issuance will not take place if these terms of use have not been accepted.
    - Maintaining certificates for their whole validity period (termination, revocation).
    - Archiving copies of the submitted documentation and the contracts duly signed by the applicants, in compliance with the certification policies published by the OSCEPA and with the legislation in force.

Therefore, RAs are liable for the consequences of their registration tasks not being carried out and agree to respect the OSCEPA's internal regulations (CPS), which must be read thoroughly by the RAs and act as a reference manual.

In the event of a claim by a Subject, entity or User, the CA must provide proof of its diligence and if it is proven that the origin of the claim lies in a data validation or verification error, the CA may hold the RA liable for the consequences, by virtue of the agreements signed with the RAs. Although, legally, the CA is the liable legal person before the Subject, entity or User, and although it therefore holds a civil liability insurance policy, according to the legally binding agreement and policies, the RA is contractually obligated to "correctly identify and authenticate the Applicant and, if applicable, the corresponding Entity", and must therefore respond to any non-fulfilment before the OSCEPA.

Of course, it is not the OSCEPA's intention to pass on the burden of assumed liability to RAs for possible damage caused by non-fulfilment of the tasks delegated to the RAs. For this reason, like the CA, the RA will be subject to a monitoring system carried out by the OSCEPA, through

both archive monitoring and conservation procedures for the archives assumed by the RA through audits to evaluate the resources used and the knowledge and monitoring of the operative procedures needed to offer RA services, among other elements.

The same liabilities must be assumed by the RAs in the event of non-fulfilment by its delegated entities, such as the in-person verification points (PVP), without prejudice to their right to proceed against them.

9.6.3. Subscriber's obligations and liability

9.6.3.1. Signatory/Subscriber

The Signatory/Subscriber will be obligated to comply with the provisions of the regulations in force and:

- To use the certificate in accordance with the provisions of this CPS and the applicable certification policies.
- To respect the provisions of the documents signed with the OSCEPA and the RA.
- To provide notification as soon as possible of the existence of any cause for revocation.
- To notify of any inaccuracy or change in the details provided to create the certificate while the certificate is valid.
- Not to use the private key or the certificate when its revocation is requested or notified by the OSCEPA or RA, or after its validity period.
- To use the digital certificate in line with its personal, non-transferable character, and therefore accept liability for any action that breaches this obligation, and to fulfil the obligations specified in the regulations applicable to digital certificates.
- To authorise the OSCEPA to proceed to process the personal data contained in the certificates, in connection with the purposes of the electronic relationship, and, in any case, to fulfil the legal obligations relating to certificate verification.
- To make sure that all information included via any means in the certificate application and the certificate itself is accurate and complete for the purpose of the certificate and that it is up to date at all times.
- To inform the corresponding certification service provider immediately of any inaccuracy detected in the certificate once it has been issued and of any changes to the information provided for the certificate to be issued.
- In the case of the loss of a physical device containing a certificate, to report this via a reliable means to the entity that issued the certificate as soon as possible and, in any event, within 24 hours of the occurrence of this circumstance, regardless of the specific event that caused it or the action that could be taken.
- Not to use the private key, the electronic certificate or any other technical medium provided by the corresponding certification service provider to carry out any transaction prohibited by the applicable legislation.

In the case of a qualified certificate, the Subscriber or certificate holder must use the key pair exclusively for the creation of electronic signatures or stamps and in accordance with any other restrictions of which it is notified.

Likewise, they must be especially diligent in the handling of their private key and secure signature creation device, in order to avoid any unauthorised use. They will be the only liable party before third parties, or before the entity they are representing if they are not authorised to do so, for the consequences of misuse or for poorly controlled use.

If the Subscriber generates their own keys, they are obligated:

- To generate their Subscriber keys using an algorithm recognised as acceptable for a qualified electronic signature or stamp.
- To create the keys within the signature or stamp creation device, using a secure device when necessary.
- To use key lengths and algorithms recognised as acceptable for a qualified electronic signature or stamp.

9.6.3.2. Certificate applicant

The applicant (either directly or through an authorised third party) seeking a certificate will be obligated to fulfil the provisions of the regulations and:

- To provide the RA with the necessary information needed to carry out the identification process.
- To guarantee the accuracy and authenticity of the information provided.
- To notify of any change in the details provided to create the certificate while the certificate is valid.
- To store their private key diligently.

9.6.3.3. Entity

In the case of certificates that involve a link to an entity, the entity is obligated to request the certificate be suspended/revoked by the RA when the Subject/Signatory ends this relationship with the organisation.

9.6.4. Third parties' obligations and liability

The User will be obligated to comply with the provisions of the regulations in force and:

- To check the validity of the certificate before carrying out any certificate-based operation. The OSCEPA provides various mechanisms to make this check, such as access to revocation lists and online consultation services such as OCSP. All these mechanisms are described on the OSCEPA's website. In particular, to make sure they are dealing with a qualified certificate, they must check it against the TLS valid at the time.

- To be familiar with and abide by the applicable guarantees, limits and liabilities involved in the acceptance and use of the certificates on which they rely. For legal person representative certificates that involve a relationship of representation based on special notarial power or a private document with limited powers, third parties must check the limits of these powers.
- To check the validity of the qualification of a signature associated with a certificate issued by the OSCEPA by checking that the Certification Authority that issued the certificate is published on the corresponding national supervisory body's trusted list.

9.6.5. Other participants' obligations and liability

Does not aplly

9.7. Exemption from liability

According to the legislation in force, the OSCEPA's and the RA's liability does not extend to situations in which the misuse of the certificate originates in conduct attributable to the Subject or the User for:

- Not providing the appropriate information initially or later on as a consequence of changes to the circumstances reflected in the electronic certificate, when this inaccuracy has not been detected by the certification service provider;
- Being negligent in terms of keeping the signature creation details and maintaining their confidentiality;
- Not requesting the revocation of the electronic certificate data in the event of doubts as to whether it has been kept confidential or not;
- Using the signature after the end of the electronic certificate's validity period;
- Surpassing the limits established in the electronic certificate.
- Conduct attributable to the User, if they act in a negligent manner, for example: if they do not check or consider the restrictions that appear on the certificate in terms of possible uses and limits on transaction amounts, or if they do not take the certificate's validity status into account.
- Damage caused to the Subject or Relying Parties due to the inaccuracy of the information that appears on the electronic certificate, if this information has been certified through a public document, recorded on a public register if required.
- Misuse or fraudulent use of the certificate, should the Subject/Holder have transferred it or authorised a third party to use it by virtue of a judicial transaction such as a mandate or an authorisation. In this case, the Subject/Holder is responsible for safeguarding the keys associated with their certificate.

The OSCEPA and the RAs will not be liable under any circumstances in any of the following situations:

- A state of war, natural disaster or any other case of force majeure.
- The use of certificates beyond the provisions of the regulations in force and certification policies.
- The misuse or fraudulent use of certificates or CRLs issued by the CA.
- The use of information contained in the certificate or CRL.
- Damage caused during the period in which the causes for revocation are checked.
- The content of digitally signed or encrypted documents or messages.
- The non-recovery of documents encrypted with the Subject's public key.

9.8. Limitation of liability in the event of transaction exchange losses

The upper limit allowed by OSCEPA in financial transactions is 0 (zero) euros.

9.9. Indemnities

See section9.2

9.10. Term and termination

9.10.1. Term

See section 5.8

9.10.2. Termination

See section 5.8

9.10.3. Effect of termination and survival

See section 5.8

9.11. Individual notifications and communication with participants

Any notification regarding this CPS will be made by email or through registered post sent to any of the addresses mentioned in the 1.5.2. contact details section.

9.12. Amendments

9.12.1. Amendment procedure

The CA reserves the right to amend this document for technical reasons or to reflect any changes in procedure that have occurred due to legal or regulatory requirements (eIDAS, national supervisory bodies, etc.) or as a result of the optimisation of the work cycle. Every new version of this CPS replaces all previous versions, which, however, remain applicable to the certificates issued while those versions were valid until the certificates' earliest expiry date. At least one update will be published annually. These updates will be reflected in the version table.

Changes made to this CPS do not require notification unless they directly affect the certificate Subject's/Signatory's rights, in which case they may submit their comments to the policy administration organisation within 15 days following publication.

9.12.2. Notification mechanism and periods

9.12.2.1. List of elements

Any element of this CPS may be changed without warning.

9.12.2.2. Notification mechanism

All proposed changes to this policy will be published immediately on the OSCEPA website:

https://www.signaturaelectronica.ad/jerarquia-politiques-i-practiques-de-certificacio

This document contains a changes and versions section, which details the changes made to it since it was created and the dates of these changes.

9.12.2.3. Comment period

Affected Signatories/Subscribers and Relying Parties may submit their comments to the policy administration organisation within **15 days** following reception of notification. The policies set this period of 15 days.

9.12.2.4. Comment processing mechanism

Any action taken as a result of a comment is subject to the PA's discretion.

9.12.3. Circumstances under which OID must be changed

Does not aplly

9.13. Dispute resolution procedure

Any dispute or conflict that may arise from this document will be dissolved definitively through legal arbitration taken on by an arbitrator, within the la Llei 13/2018, del 31 de maig, del Tribunal d'Arbitratge del Principat d'Andorra to which the administration of the arbitration and the designation of an arbitrator or an arbitration court are assigned. The parties agree to comply with the final decision.

9.14. Applicable legislation

The execution, interpretation, modification and validity of this CPS are governed by current Andorran legislation and current European legislation.

9.15. Compliance with applicable legislation

See point 9.14

9.16. Miscellaneous provisions

9.16.1. Entire agreement

The holders and Relying Parties accept this Practice Statement and the certification policies in their entirety.

9.16.2. Assignment

The parties to this CPS cannot transfer any of their rights or obligations under this CPS or applicable agreements without the OSCEPA's written consent.

9.16.3. Severability

If some individual provisions of this CPS prove to be ineffective or incomplete, this will not affect the validity of the other provisions.

The ineffective provision will be replaced by an effective one that is deemed to reflect the meaning and purpose of the ineffective provision more closely. In the case of incomplete provisions, an amendment will be made that is deemed to correspond to what would reasonably have been agreed upon in accordance with the meaning and purposes of this CPS, if the issue had been considered beforehand.

9.16.4. Enforcement (lawyers' fees and waiver of rights)

The OSCEPA may request an indemnity and lawyers' fees from a party due to damage caused and expenses relating to the conduct of this party. Even if the OSCEPA should fail to invoke a provision of this CPS at some point, the OSCEPA may still enforce this provision later on or any other provision of this CPS. To take effect, any renunciation must be made in writing and signed by the OSCEPA.

9.16.5. Force majeure

Force majeure clauses, if there are any, are included in the "Subscriber agreement".

9.17. Other provisions

9.17.1. Publication and copying of the policy

A copy of this CPS will be available in electronic format at the following address: https://www.signaturaelectronica.ad/jerarquia-politiques-i-practiques-de-certificacio

9.17.2. CPS approval procedures

The publication of revised versions of this CPS must be approved by the OSCEPA Policy Authority.

The OSCEPA publishes every new version on its website. The CPS is published in PDF format signed electronically by the OSCEPA.

10. APPENDIX I: Document history

Date	Version	Purpose
October 2013	V1.0	**Versió inicial**
November 2017	V1.0	**Revisió**
Octob er 2019	V2.0	**Canvi d'ordre, denominació i desenvolupament en diversos punts per alinear-se amb l'RFC3647**
February 2020	V2.1	**Canvi de sintaxis**
March-April 2020	V2.2	**Revisió CPS**
July 2021	v2.3.2	**Identification of a person's identity: new wording to integrate all the identification methods provided for by the eIDAS regulation and national standards**
August 2021	v2.3.3	**Issuing certificates to Minors under 16 and between 16-18**
February 2022	V3.0	**Audit eIDAS**