CERTIFICATION PRACTICE STATEMENT ANDORRAN PUBLIC ADMINISTRATION PKI

Govern d'Andorra

Version 2.3.2

Language: **English**

Table of Contents

1. INTRODUCTION 8

1.1. Overview 8

1.2. Document name and identification 8

1.3. PKI participants 8

1.3.1. Certification Authorities 8
1.3.2. Registration Authorities 8
1.3.3. Signatory/Subscriber 9
1.3.4. Relying Party 9
1.3.5. Other participants 9

1.4. Scope of application and uses 9

1.4.1. Appropriate uses of certificates 9
1.4.2. Forbidden uses of certificates 9

1.5. Policy Authority 10

1.5.1. Organisation administering the document 10
1.5.2. Organisation contact details 10
1.5.3. Person determining CPS's suitability for the policy 10
1.5.4. Document management procedures 10

1.6. Acronyms and definitions. 10

1.6.1. Acronyms 10
1.6.2. Definitions 11

2. RESPONSIBILITY FOR PUBLICATION AND REPOSITORIES 13

2.1. Repositories 13

2.2. Publication of certificate information 13

2.3. Frequency of publication 13

2.4. Repository access control 13

3. IDENTIFICATION AND AUTHENTICATION 14

3.1. Naming 14

3.1.1. Types of name 14
3.1.2. Meaning of names 14
3.1.3. Anonymity or Subscriber pseudonyms 14
3.1.4. Rules used to interpret different name formats 14
3.1.5. Uniqueness of names 14
3.1.6. Issuance of various natural person certificates for one holder 14
3.1.7. Recognition, authentication and function of trademarks and other distinctive signs 14
3.1.8. Name dispute resolution procedure 14

3.2. Initial identity validation 14

3.2.1. Entity identification 15
3.2.2. Identification of an individual's identity 15
3.2.3. Non-verified Subscriber information 16
3.2.4. Authority validation 17
3.2.5. Criteria for interoperation 18

3.3. Identification and authentication of re-key requests 18

3.3.1. Validation for routine certificate re-key 18
3.3.2. Identification and authentication of a re-key request following a revocation 18

3.4. Identification and authentication of revocation request 18

4. OPERATIONAL REQUIREMENTS FOR CERTIFICATE LIFE CYCLE 19

4.1. Certificate application 19
4.1.1. Who can request a certificate? 19
4.1.2. Registration procedure and responsibilities 19

4.2. Certificate application processing 19
4.2.1. Execution of identification and authentication functions 19
4.2.2. Approval or rejection of application 19
4.2.3. Time to process application 20

4.3. Certificate issuance 20
4.3.1. CA actions during the issuing process 20
4.3.2. Notification of issuance to the Subscriber 21

4.4. Acceptance of certificates 21
4.4.1. Conduct that constitutes acceptance of the certificate 21
4.4.2. Publication of certificate by the CA 21
4.4.3. Certificate issuing notification from CA to other entities 21

4.5. Use of key pair and certificates 21
4.5.1. Subscriber's use of certificate and private key 21
4.5.2. Relying Party's use of public key and certificate 22

4.6. Renewal of certificate 22
4.6.1. Circumstances for certificate renewal 22
4.6.2. Who can request a renewal? 22
4.6.3. Certificate renewal request processing 22
4.6.4. New issuance notification to the Subscriber 23
4.6.5. Conduct that constitutes acceptance of the renewal certificate 23
4.6.6. Publication of renewal certificate by the CA 23
4.6.7. Certificate issuing notification from CA to other entities 23

4.7. Certificate re-key 23
4.7.1. Circumstances for certificate re-key 23
4.7.2. Who can request the certification of a new public key? 23
4.7.3. Processing certificate re-keying requests 23
4.7.4. New issuance notification to the Subscriber 23
4.7.5. Conduct that constitutes acceptance of a re-keyed certificate 23
4.7.6. Publication of re-keyed certificate by the CA 23
4.7.7. Certificate issuing notification from CA to other entities 23

4.8. Modification of certificates 24
4.8.1. Circumstances for certificate modification 24
4.8.2. Who can request a certificate modification? 24
4.8.3. Processing certificate modification requests 24
4.8.4. New certificate issuance notification to the Subscriber 24
4.8.5. Conduct that constitutes acceptance of the modified certificate 24
4.8.6. Publication of modified certificate by the CA 24
4.8.7. Certificate issuing notification from CA to other entities 24

4.9. Revocation and suspension of certificates 24
4.9.1. Reasons for revocation 25
4.9.2. Who can request a revocation? 25
4.9.3. Revocation request procedure 26
4.9.4. Grace period for revocation request 26
4.9.5. Deadline for CA to process the revocation request 26
4.9.6. Revocation check requirements for Relying Parties 26
4.9.7. Frequency with which CRLs are issued 26
4.9.8. Maximum latency for CRLs 26
4.9.9. Availability of online revocation check 26
4.9.10. Requirements for online revocation check 27
4.9.11. Other available ways to find out revocation information 27
4.9.12. Special requirements for revocation due to compromised keys 27

4.9.13. Circumstances for suspension 27
4.9.14. Who can request a suspension? 27
4.9.15. Suspension request procedure 27
4.9.16. Suspension period limits 27
4.10. Certificate status checking services 27
4.10.1. Operational characteristics 27
4.10.2. Service availability 27
4.10.3. Optional characteristics 27
4.11. End of subscription 28
4.12. Key escrow and recovery 28
4.12.1. Key escrow and recovery policy and practices 28
4.12.2. Session key encapsulation and recovery policy and practices 28
5. PHYSICAL, MANAGEMENT AND OPERATIONAL CONTROLS 29
5.1. Physical security controls 29
5.1.1. Location and construction 29
5.1.2. Physical access 29
5.1.3. Electricity supply and air conditioning 29
5.1.4. Exposure to water 29
5.1.5. Fire prevention and protection 30
5.1.6. Storage system 30
5.1.7. Waste disposal 30
5.1.8. Off-site backup 30
5.2. Procedural controls 30
5.2.1. Trusted roles 30
5.2.2. Number of people required per task 31
5.2.3. Identification and authentication for each role 31
5.2.4. Roles that require separation of duties 31
5.2.5. Starting and stopping the PKI management system 31
5.3. Personnel controls 31
5.3.1. Qualifications, experience and clearance requirements 31
5.3.2. Background check procedures 32
5.3.3. Training requirements 32
5.3.4. Retraining requirements and frequency 32
5.3.5. Frequency and sequence of task rotation 32
5.3.6. Sanctions for unauthorised actions 32
5.3.7. Personnel hiring requirements 32
5.3.8. Documentation provided to personnel 32
5.4. Event recording procedures 33
5.4.1. Types of event recorded 33
5.4.2. Frequency with which audit logs are processed 33
5.4.3. Retention period for audit logs 33
5.4.4. Protection of audit logs 33
5.4.5. Audit log backup procedures 34
5.4.6. Audit information collection system 34
5.4.7. Notification to event-causing subject 34
5.4.8. Vulnerability analysis 34
5.5. Record archival 34
5.5.1. Type of records archived 34
5.5.2. Archive retention period 34
5.5.3. Archive protection 35
5.5.4. Archive backup procedures 35
5.5.5. Requirements for record time-stamping 35
5.5.6. Audit information collection system 35

5.5.7. Procedures for obtaining and verifying archived information 35
5.6. Key changeover 35
5.7. Recovery in event of compromised key or disaster 35
5.7.1. Compromised key or incident management procedures 35
5.7.2. Corruption of resources, applications or data 35
5.7.3. Entity's private key compromised 35
5.7.4. Business continuity following a disaster 36
5.8. Termination of CA or RA 36
6. TECHNICAL SECURITY CONTROLS 37
6.1. Key pair generation and installation 37
6.1.1. Key pair generation 37
6.1.2. Delivery of private key to Subscriber 37
6.1.3. Delivery of public key to certificate issuer 37
6.1.4. Delivery of public key from CA to Relying Parties 37
6.1.5. Size of keys 37
6.1.6. Public key generation parameters and quality assurance 37
6.1.7. Purpose of the use of keys 37
6.2. Protection of private key and standards for cryptographic modules 38
6.2.1. Controls and standards for cryptographic modules 38
6.2.2. Multi-person control (n out of m) of private key 38
6.2.3. Private key escrow 38
6.2.4. Private key backup 38
6.2.5. Private key archival 38
6.2.6. Entering the private key in the cryptographic module 39
6.2.7. Storing the private key in the cryptographic module 39
6.2.8. Private key activation method 39
6.2.9. Private key deactivation method 39
6.2.10. Private key destruction method 39
6.2.11. Cryptographic module capabilities 39
6.3. Other aspects of key pair management 39
6.3.1. Public key archival 39
6.3.2. Period of use for public and private keys 39
6.4. Activation data 39
6.4.1. Generation and activation of activation data 40
6.4.2. Protection of activation data 40
6.4.3. Other aspects of activation data 40
6.5. Computer security controls 40
6.5.1. Specific computer security technical requirements 40
6.5.2. Assessment of computer security 40
6.6. Life cycle security controls 40
6.6.1. System development controls 41
6.6.2. Security management controls 41
6.6.3. Life cycle security evaluation 42
6.7. Network security controls 42
6.8. Time-stamping 43
7. CERTIFICATE, CRL AND OCSP PROFILES 44
7.1. Certificate profile 44
7.1.1. Version number 44
7.1.2. Certificate extensions 44
7.1.3. Algorithm object identifiers (OID) 44

7.1.4. Name format 44
7.1.5. Name restrictions 44
7.1.6. Certification policy object identifier (OID) 44
7.1.7. Use of "Policy Constraints" extension 44
7.1.8. Policy qualifiers syntax and semantics 44
7.1.9. Processing semantics for the critical "Certificate Policy" extension 44

7.2. CRL profile 44
7.2.1. Version number 45
7.2.2. CRL and extensions 45

7.3. OCSP profile 45
7.3.1. Version number 45
7.3.2. OCSP extensions 45

8. COMPLIANCE AUDITS 46

8.1. Frequency or circumstances of audits 46
8.1.1. Audits at Registration Authorities 46

8.2. Identification and name of auditor 46

8.3. Relationship between auditor and CA 46

8.4. Topics covered by audit 46

8.5. Action taken as a result of deficiencies 47

8.6. Communication of results 47

9. LEGAL ASPECTS AND OTHER ISSUES 48

9.1. Fees 48
9.1.1. Certificate issuance and renewal fees 48
9.1.2. Certificate access fees 48
9.1.3. Fees for access to information on status of certificates or revoked certificates 48
9.1.4. Fees for access to the contents of these Certification Practices. 48
9.1.5. Refund policy 48

9.2. Financial liability 48
9.2.1. Insurance cover 48
9.2.2. Other assets 48
9.2.3. Insurance or guarantee for end entities 48

9.3. Confidentiality of business information 48
9.3.1. Type of information to be kept confidential 48
9.3.2. Type of information considered non-confidential 48
9.3.3. Duty to protect confidential information 48

9.4. Privacy of personal information 49
9.4.1. Privacy plan 49
9.4.2. Information treated as private 49
9.4.3. Information not considered private 49
9.4.4. Duty to protect private information 49
9.4.5. Notice and consent to use private information 49
9.4.6. Disclosure pursuant to judicial or administrative proceedings 49
9.4.7. Other information disclosure circumstances 49

9.5. Intellectual property rights 49

9.6. Obligations and civil liability 49
9.6.1. CA's obligations and liability 49
9.6.2. RA's obligations and liability 50
9.6.3. Subscriber's obligations and liability 51
9.6.4. Third parties' obligations and liability 52

9.6.5. Other participants' obligations and liability 52
9.7. Exemption from liability 52
9.8. Limitation of liability in the event of transaction exchange losses 53
9.9. Indemnities 53
9.10. Term and termination 53
9.10.1. Term 53
9.10.2. Termination 53
9.10.3. Effect of termination and survival 53
9.11. Individual notifications and communication with participants 53
9.12. Amendments 53
9.12.1. Amendment procedure 53
9.12.2. Notification mechanism and periods 54
9.12.3. Circumstances under which OID must be changed 54
9.13. Dispute resolution procedure 54
9.14. Applicable legislation 54
9.15. Compliance with applicable legislation 54
9.16. Miscellaneous provisions 54
9.16.1. Entire agreement 54
9.16.2. Assignment 54
9.16.3. Severability 54
9.16.4. Enforcement (lawyers' fees and waiver of rights) 54
9.16.5. Force majeure 54
9.17. Other provisions 54
9.17.1. Publication and copying of the policy 54
9.17.2. CPS approval procedures 55
1. APPENDIX I: document history 56

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. This document identifies the practices and procedures followed by the Office for Electronic Trust Services of the Principality of Andorra – hereinafter OSCEPA – when issuing digital certificates within this infrastructure.

These practices are aligned with the requirements set out in version 1.6.6 of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates established by the CA/B Forum http://www.cabforum.org.

Should there be any inconsistencies between this document and the Baseline Requirements, the Baseline Requirements will prevail.

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 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

1.3.1. **Certification Authorities**

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:

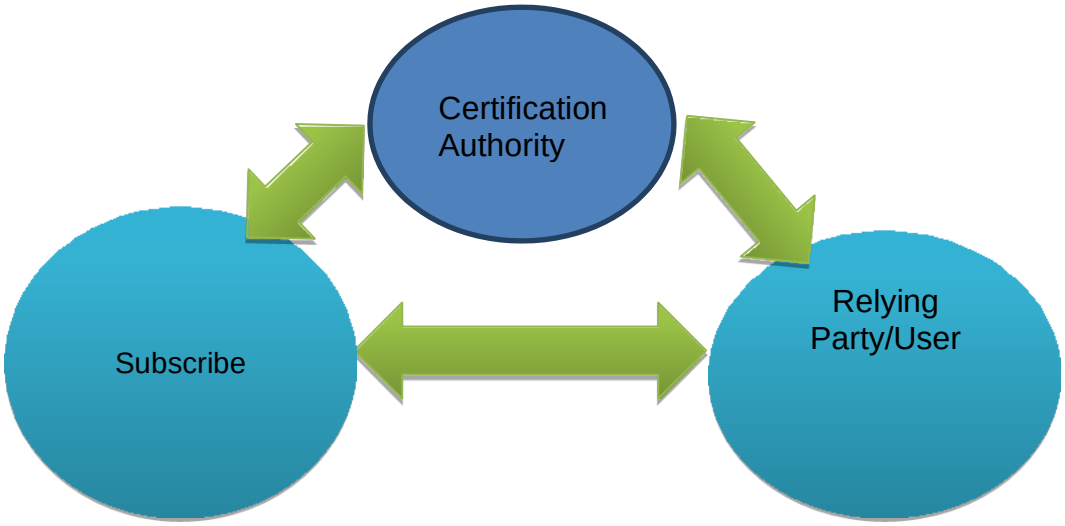
- The Certification Authority itself.
- Any national or international agent that maintains a contractual relationship with the CA and that goes through the registration and audit procedures that demonstrate that it fulfils the requirements set out in this document.

1.3.3. **Signatory/Subscriber**

The Signatory/Subscriber is considered the holder of the certificate, when the holder is a natural or legal person and is described in the CN field of the certificate. When a certificate is issued in the name of a hardware device or computer application, the natural or legal person requesting the certificate will be considered the Signatory/Subscriber.

1.3.4. **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.



1.3.5. **Other participants**

Not applicable.

1.4. Scope of application and uses

1.4.1. **Appropriate uses of certificates**

OSCEPA certificates may be used under the terms set out in this document. In general terms, certificates may be used for the following purposes:

- Authentication based on X.509v3 certificates.
- An advanced or recognised electronic signature, based on X.509v3 certificates.
- Asymmetric or mixed encryption, based on X.509v3 certificates.

1.4.2. **Forbidden uses of certificates**

Certificates may only be used with the restrictions and for the purposes with which they have been issued in each case. These restrictions and purposes are described in this document.

Certificates are not designed, cannot be used and are not authorised to be used or resold as control equipment for dangerous situations or for uses that require fail-safe actions, such as the running of nuclear facilities, navigation systems, air traffic communication systems or arms control systems, where an error could directly cause death, personal injury or serious environmental damage.

The use of digital certificates for transactions that contravene the CPS or the CA's contracts

with RAs or with Signatories/Subscribers will be considered inappropriate usage, with all corresponding legal effects, and the CA will be exempt from all liability for the Signatory's or any third party's inappropriate use of the certificate, pursuant to the legislation in force.

The OSCEPA does not have access to the data to which the use of a certificate may be applied. Therefore, as a consequence of this technical impossibility of accessing the content of the message, the OSCEPA cannot make any assessment whatsoever of this content; the Signatory will therefore bear any liability arising from the content linked to the use of a certificate. Furthermore, the Signatory will take on any liability deriving from the use of the certificate outside of the restrictions and conditions of use set out in the CPS and in the contracts between the CA and its Signatories, as well as from any other inappropriate use of the certificate under the terms of this section or that may be interpreted as such in accordance with the legislation in force.

In the certificate, the OSCEPA incorporates information on usage restrictions, whether through standardised fields in the "key usage", "basic constraints" and/or "name constraints" attributes, which are marked as critical in

the certificate and therefore must be filled by the applications using it, or through limitations to the attributes such as “extended key usage” and/or through texts incorporated in the “user notice” field, which are marked as “non-critical” but must nonetheless be filled by the holder and the User of the certificate.

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 technical management.

1.5.2. **Organisation contact details**

Address:	Carrer de la Grau, Edifici Prat del Rull, Andorra la Vella
Telephon	+376 875700
e: 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 technical 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 certificate information

The OSCEPA publishes CRLs and access to the OCSP service at:

http://crl.govern.ad/GovernAndorra.crl http://crl1.govern.ad/GovernAndorra.crl http://ocsp.govern.ad

2.3. Frequency of publication

The OSCEPA issues and publishes revocation lists periodically in accordance with the table in the "Frequency with which CRLs are issued" section of these practices.

On its website https://www.signaturaelectronica.ad/jerarquia-politiques-i-practiques-de-certificacio,the OSCEPA immediately publishes any modification to its policies and the CPS, and provides a record of past versions.

This information will be published as soon as it becomes available and, especially, immediately when amendments regarding certificate validity are made.

Any changes made to the CPS will be governed by the provisions of the corresponding section of the CPS.

Information on certificates' revocation status will be published in accordance with the provisions of the corresponding section of the CPS.

Fifteen (15) days after the new version is published, the reference to the change on the home page may be removed and inserted into the repository. Old versions of the documentation will be preserved for a period of fifteen (15) years by the Certification Entity and may be consulted by interested parties who provide a reason for the consultation.

2.4. Repository access control

Access to the OSCEPA repository is free.

Physical and logical controls are maintained to prevent any modifications or unauthorised erasure of information in the repository.

3. IDENTIFICATION AND AUTHENTICATION

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**

Not applicable.

3.1.4. **Rules used to interpret different name formats**

In all cases, the OSCEPA follows the provisions of the X.500 reference standard in the ISO/IEC 9594.

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.

3.1.6. **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.

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

The OSCEPA does not take on any commitments regarding the use of trademarks and other distinctive signs when issuing certificates. The OSCEPA deliberately prohibits the use of a distinctive sign which the Signatory/Subject does not have the right to use. However, the Andorran Public Administration is not obligated to look for evidence regarding rights of use of trademarks or other distinctive signs before issuing certificates, so it can refuse to generate or request the revocation of any certificate involved in a dispute.

3.1.8. **Name dispute resolution procedure**

The OSCEPA accepts no liability in the event of a name dispute. In any case, names are assigned in the order in which they are received.

The Andorran Public Administration shall not mediate in this kind of dispute; it must be resolved directly between the parties.

3.2. Initial identity validation

Methods to prove possession of private key

The OSCEPA uses various circuits for issuing certificates where the private key is managed differently. The private key can be generated either by the User or by the OSCEPA.

a) Generation of keys by the OSCEPA

In software: They are delivered to the Subject/Signatory physically or via email through protected files using the PKCS#12 standard. The process is guaranteed to be secure as the access code for the PKCS#12 file needed for installation in applications is delivered via a different means to that used to deliver the file.

In hardware: The keys may be delivered by the OSCEPA to the Subject/Signatory directly or via a Registration Authority on a secure signature creation device.

b) Generation of keys by Subscriber

The Signatory has use of a key generation mechanism, either through software or hardware. The proof of possession of the private key in these cases is the request received by the OSCEPA in PKCS#10 or a cryptographically equivalent format.

3.2.1. Entity identification

3.2.1.1. Identity

Prior to the issuance and delivery of a certificate for a legal person or a natural person linked to an entity, data relating to the constitution and the legal personality of the entity must be authenticated.

In all cases, for these certificates, entity identification is required, for which the RA will require the relevant documentation according to the type of entity.

The following will also be checked:

- That the information or documents provided are no older than 1 year.

For public administrations: No documentation is required to prove the existence of a public law entity, body or public administration, as their identity is part of the corporate area of the State's public administrations.

3.2.1.2. Trademarks

See point 3.1.6

3.2.1.3. Country verification

See point 3.2.2.1

3.2.1.4. Validation of domain authorisation or control

See point 3.2.5.1

3.2.1.5. Authentication of IP address

Not applicable.

3.2.1.6. Wildcard domain validation

Not applicable.

3.2.1.7. Accuracy of data sources

See point 3.2.2.1

3.2.1.8. CAA records

Not applicable.

3.2.2. Identification of an individual's identity

Prior to the issuance and delivery of a certificate, verification of the identity of the applicant is required, presenting the original in force of one of the following documents:

a) • Andorran nationality:
   a. ➢Passport.

b) • Foreigners:
   a. ➢Residence card or passport or identity document of the Holder's country and Tax Registration Number (NRT).

For foreign identity documents, a sworn translation may be requested if necessary.

Certificates may not be issued to non-emancipated minors of 16 years, totally or partially legally incapacitated, or when there are substantiated suspicions that the applicant is not in possession of their full mental abilities.

Methods of identification: the identity of an individual may be verified using any of the methods in accordance with the provisions of article 26 of Law 35/2014, of 27 November, on electronic trust services, or which marks the eIDAS Regulation and in accordance with national law:

1. Physical presence: the presence of the Applicant is required before an operator of the Certification Authority, the Registration Authority or the Face-to-Face Verification Point.
2. At a distance, using electronic means of identification, for which the presence of the natural person or an authorized representative of the legal person has been guaranteed prior to the issuance of the qualified certificate, and which meet the established requirements with Article 8 (of the eIDAS

Regulation) regarding “substantial” or “high” levels of security. Electronic identification systems notified by Member States under Article 9.1 of the eIDAS Regulation will be accepted. Electronic national identity documents will be accepted.

3. By means of another qualified certificate issued by the CA of the Office of Electronic Trust Services of the Principality of Andorra or by another CA, for which the physical presence or a means of identification would have been used notified electronic, for the identification of the applicant, provided that it is clear to the provider that the presence occurred less than five years ago.
4. Using other methods of identification recognized at national or European level that provide equivalent security in terms of reliability to the physical presence. Equivalent safety will be confirmed by a conformity assessment body.
   The Electronic Trust Services Office of the Principality of Andorra has a Video Identification method (IDVideo) based on the video-conferencing procedure authorized by the Executive Service of the Commission for the Prevention of Money Laundering and Monetary Offenses in the member states of the European Union for the issuance of qualified certificates.
   Brief description of IDVideo:
   - Requires applicants to be equipped with a device with internet access (PC, Tablet, smartphone, etc.), a camera and a sound system.
   - The operator must connect with the applicant synchronously to proceed with the live identity verification.
   - The applicant must follow the operator's instructions, answer the questions asked, agree to have their image recorded during the session, show the identity document for all faces or pages that are necessary for the operator can keep a copy.
   - The operator will proceed to the validation of the applicant's proof of life and facial recognition coinciding with the identity document.
   - The whole process is recorded so that it can be audited.
   - Registration data, ie audio and video files and structured metadata in electronic format, are stored in a protected manner and in accordance with the European standard on the protection of personal data.
   - For security and fraud prevention reasons, only conventional identity documents will be accepted under this method of identification (Passport of the applicant's country of origin or official identity document). The identification of foreign applicants residing in Andorra may be authorized by the Certification Authority after reviewing the objective characteristics of their identity documents in terms of certainty of identification, security of the Issuing Authority and specific training.

This method of identification by video-conference may be used to issue qualified electronic certificates provided that it complies with the applicable technical conditions and requirements, established by the Supervisory Body in the conditions it issues.

3.2.3. **Non-verified Subscriber information**

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

3.2.4. Authority validation

3.2.4.9. Identification of affiliation

Type of certificate	Documentation
Individual natural person certificates 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	Article 26.2 of Law 35/2014, of 27 November, on electronic trust services states the following: “The qualified electronic trust service provider must reliably verify the identity and, where applicable, any other specific attribution of the natural person to whom the qualified electronic certificate is issued, by displaying the public or private documents that it sufficiently accredits. This information must be verified by the qualified service provider or by a third party acting under the responsibility of the qualified service provider: i. Through the physical presence of that person, or ii. Remotely, using other recognized electronic certificates issued by a qualified service provider or By means of a qualified electronic signature certificate or a qualified electronic stamp delivered in accordance with sections a and b, or By means of other methods of identification recognized at national level that give a guarantee equivalent to the reliability of the presence of the natural person. Equivalence in the level of reliability and safety shall be certified by a conformity assessment body. " On the other hand, article 26.3 of Law 35/2014, of 27 November, on electronic trust services, establishes that in the case of "electronic certificates issued to natural persons but linked to an organization, entity, institution, company or other legal person, the trusted service provider must prove, in addition to the identity of the applicant and the person identified in the electronic certificate, the data relating to the constitution and legal personality of the company. entity, or the extension and validity of the powers or powers of representation of the applicant, by means of the public documents that it accredits of specific form or by means of the consultation of the corresponding public registry, that is the result of the data that have to be included ".

Public law entity, body or public administration stamp Company stamp (legal person)	Article 26.2 of Law 35/2014, of 27 November, on electronic trust services states the following: “The qualified electronic trust service provider must reliably verify the identity and, where applicable, any other specific attribution of the natural person to whom the qualified electronic certificate is issued, by displaying the public or private documents that it sufficiently accredits. This information must be verified by the qualified service provider or by a third party acting under the responsibility of the qualified service provider: i. Through the physical presence of that person, or ii. Remotely, using other recognized electronic certificates issued by a qualified service provider or By means of a qualified electronic signature certificate or a qualified electronic stamp delivered in accordance with sections a and b, or By means of other methods of identification recognized at national level that give a guarantee equivalent to the reliability of the presence of the natural person. Equivalence in the level of reliability and safety shall be certified by a conformity assessment body. " i. On the other hand, article 26.3 of Law 35/2014, of 27 November, on electronic trust services, establishes that in the case of "electronic certificates issued to natural persons but linked to an organization, entity, institution, company or other legal person, the trusted service provider must prove, in addition to the identity of the applicant and the person identified in the electronic certificate, the data relating to the constitution and legal personality of the company. entity, or the extension and validity of the powers or powers of representation of the applicant, by means of the public documents that it accredits of specific form or by means of the consultation of the corresponding public registry, that is the result of the data that have to be included ".

3.2.5. Criteria for interoperation

The OSCEPA may provide services that enable another CA to operate within, or interoperate with, its PKI. This interoperation may include cross certification, unilateral certification and other types of operation. The OSCEPA reserves the right to provide interoperation services and to interoperate with other CAs, the terms of which must be established in a contract.

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?

A certificate application may be submitted by the Subject of the certificate or by an authorised representative.

4.1.2. Registration procedure and responsibilities

4.1.2.1. Online forms

Certificate applications are generally made through access to application forms on the website below, through a link to a specific form sent to the applicant, or in person at any Registration Entity.

https://www.signaturaelectronica.ad

The website contains the forms needed to make a request for any type of certificate distributed by the OSCEPA in various formats, as well as signature generation devices, if necessary.

The form can include a CSR (PKCS#11), if the User has created the keys.

Following the confirmation of the application details, the User will receive an email at the address associated with the certificate application containing a link to confirm the application and accept the terms of use.

Once the request is confirmed, the Subscriber is informed of the documentation they need to present at an authorised registration office and is notified that they must comply with the in-person identification requirement, if applicable.

4.1.2.2. Requests via Web Services (WS) layer

In order to enable the integration of third-party applications with the STATUS ® certificate management platform (property of AC Camerfirma), a Web Services (WS) layer has been developed to offer certificate issuance and revocation processes. Calls to these WS are signed with a certificate recognised by the platform.

The “blind” issuance of this type of certificate requires the process to be thoroughly reviewed. Before initiating issuance through this platform, a favourable technical report from AC Camerfirma and a contract where the Registration Authority promises to maintain the system in ideal security conditions and notify the OSCEPA of any modification or incident are required. In addition, the system may be subject to annual audits, which check:

1. The documentary records of the certificates issued
2. That the certificates are being issued in accordance with the guidelines set in the certification policies by which they are governed

4.1.2.3. Batches

The STATUS platform also allows for request circuits through batches. In this case, the applicant will send the RA a file structured in accordance with a template fixed by the OSCEPA with the applicants’ details. The RA will then proceed to load the requests onto the management application.

4.2. Certificate application processing

4.2.1. Execution of identification and authentication functions

Once a certificate application has been made, the RA operator verifies that the information provided is in order by accessing the PKI management platform (STATUS or SIAVAL SafeCert).

The platform operator has an internal management certificate issued after a training and assessment process for the purpose of carrying out these operations.

The certificate used by the registration operator is considered a multi-factor authentication process used both to access the PKI management platform (STATUS or SIAVAL SafeCert) and to approve each certificate issuance application through an electronic signature.

4.2.2. Approval or rejection of application

For end entity certificates:

The registration operator views the applications that have yet to be processed and that have been assigned to them.

The RA operator waits for the Subject/Signatory to submit the corresponding documentation.

If the information is incorrect, the RA rejects the application. Should the details be verified, the Registration Authority will approve the issuance of the certificate through an electronic signature with its operator certificate.

4.2.3. **Time to process application**

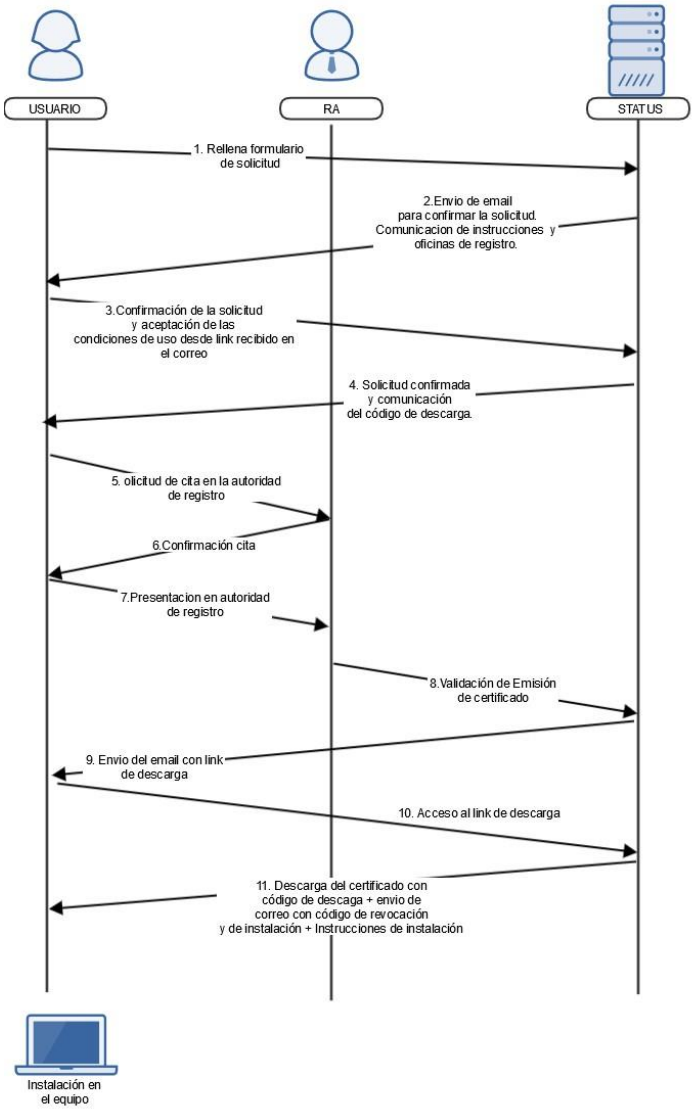
Applications submitted via the PKI STATUS platform are accepted once the accrediting documentation associated with the certificate profile is checked. Where viable, the OSCEPA will always aim to delete applications older than a year.

4.3. Certificate issuance

4.3.1. **CA actions during the issuing process**

4.3.1.1. Software certificates

Once the application is approved, the Subscriber receives an email with notification of this and can proceed to generate and download the certificate. To install it, the Subscriber will need the product code sent to them with the contract and an installation code sent in a separate email along with a revocation code.



4.3.1.2. Hardware certificates (Secure Signature Creation Device)

The private key is generated by the holder via the issuance process established by the provider, once the RA has seen and validated them.

Key pairs are generated on a qualified signature creation device or QSCD, the SIAVAL SafeCert Server Signing System. The keys are protected exclusively by the Signatory and, therefore, no private key is delivered to the holder. The protection consists of a PIN or password and a second authentication factor based on a text message sent to the User's mobile telephone.

The system will inform the holder that their centralised signature certificate is going to be issued and, at the same time, will generate a private key and store it under protection in the system, so that use of it is controlled exclusively by the holder.

The public key is generated alongside the private key on the qualified signature creation device SIAVAL SafeCert Server Signing System and is delivered to the Certification Authority via a certification application in PKCS#10 format.

4.3.2. Notification of issuance to the Subscriber

The OSCEPA will inform the applicant via email of whether the application has been approved or denied.

4.4. Acceptance of certificates

4.4.1. Conduct that constitutes acceptance of the certificate

Once the certificate is issued, the User has 7 days to check that it has been issued correctly.

If the certificate has not been issued correctly due to technical issues, the certificate will be revoked and a new one will be issued.

4.4.2. Publication of certificate by the CA

The OSCEPA offers a status consultation system for issued certificates on its website: https://secure.camerfirma.com/solicitudes_status/estado_certificado.php. Access to this page is free.

4.4.3. Certificate issuing notification from CA to other entities

The OSCEPA offers a status consultation system for issued certificates on its website: https://secure.camerfirma.com/solicitudes_status/estado_certificado.php. Access to this page is free.

4.5. Use of key pair and certificates

4.5.1. Subscriber's use of certificate and private key

Key usage limitations are defined within the certificate under the following extensions: *keyUsage*, *extendedKeyUsage* and *basicConstraints*

CA	Key Usage	Extended Key Usage	Basic Constraint
Andorran Public Administration Certification Entity	critical, cRLSign, keyCertSign	–	critical,CA:true
NATURAL PERSON on DSCF – SIGNATURE	critical, nonRepudiation	clientAuth, emailProtecti	critical,CA:false
NATURAL PERSON on DSCF – IDENTITY	critical, digitalSignature	clientAuth, emailProtecti	critical,CA:false
NATURAL PERSON WITH REGULATED PROFESSION on DSCF	critical, nonRepudiation	clientAuth, emailProtecti	critical,CA:false
NATURAL PERSON WITH REGULATED PROFESSION on DSCF	critical, digitalSignature	clientAuth, emailProtecti	critical,CA:false
NATURAL PERSON WITH REGULATED PROFESSION on DSCF – ENCRYPTED	critical, keyEncipherment,	clientAuth, emailProtecti on	critical,CA:false
NATURAL PERSON at the service of an ORGANISATION on DSCF – SIGNATURE	critical, nonRepudiation	clientAuth, emailProtecti	critical,CA:false
NATURAL PERSON at the service of an ORGANISATION on DSCF – IDENTITY	critical, digitalSignature	clientAuth, emailProtecti	critical,CA:false
NATURAL PERSON at the service of the ADMINISTRATION on DSCF – SIGNATURE	critical, nonRepudiation	clientAuth, emailProtecti	critical,CA:false
NATURAL PERSON at the service of the ADMINISTRATION on DSCF – IDENTITY	critical, digitalSignature	clientAuth, emailProtecti	critical,CA:false
NATURAL PERSON at the service of the ADMINISTRATION on DSCF – ENCRYPTED	critical, keyEncipherment,	clientAuth, emailProtecti on	critical,CA:false
COMPANY STAMP (legal person) on HSM – ELECTRONIC STAMP	critical, nonRepudiation	clientAuth, emailProtecti	critical,CA:false

COMPANY STAMP (legal person) on HSM – IDENTITY	critical, digitalSignature	clientAuth, emailProtecti	critical,CA:false
COMPANY STAMP (legal person) on SOFTWARE	critical, digitalSignature, keyEncipherment, dataEnciphermen t, nonRepudiation	clientAuth, emailProtecti on	critical,CA:false
PUBLIC LAW ENTITY, BODY OR PUBLIC ADMINISTRATION STAMP on HSM – SIGNATURE	critical, nonRepudiation	clientAuth, emailProtecti on	critical,CA:false
PUBLIC LAW ENTITY, BODY OR PUBLIC ADMINISTRATION STAMP on HSM – IDENTITY	critical, digitalSignature	clientAuth, emailProtecti on	critical,CA:false
PUBLIC LAW ENTITY, BODY OR PUBLIC ADMINISTRATION STAMP on SOFTWARE	critical, digitalSignature, keyEncipherment, dataEnciphermen t, nonRepudiation	clientAuth, emailProtecti on	critical,CA:false
REPRESENTATIVE OF LEGAL PERSON on HSM – ELECTRONIC SIGNATURE	critical, nonRepudiation	clientAuth, emailProtecti on	critical,CA:false
REPRESENTATIVE OF LEGAL PERSON on HSM – IDENTITY	critical, digitalSignature	clientAuth, emailProtecti on	critical,CA:false

Although it is technically possible to encrypt data with the certificates, the OSCEPA accepts no responsibility for any damage caused by the owner's loss of control of the private key needed to decrypt the information.

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

The Relying Parties must access and use the public key and the certificate in accordance with the provisions of this CPS and of the "Terms of Use", having consulted a physical document or accepted them in the issuance process.

4.6. Renewal of certificate

4.6.1. Circumstances for certificate renewal

Certificates must be renewed before their expiry date. The OSCEPA will issue the renewed certificate with a start date that corresponds to the old certificate's expiry date.

OCSP certificates are issued periodically and are not subject to renewal processes.

4.6.2. Who can request a renewal?

For certificates eligible for renewal, the holder is authenticated through the certificate to be renewed.

4.6.3. Certificate renewal request processing

Before a certificate is renewed, the OSCEPA checks that the information used to verify the Signatory's and the key holder's identity and other details is still valid.

In the case of the renewal of natural person end entity certificates, a certificate may be issued without the person being physically present for a period of 5 years starting from the last time they were registered in person. After this time, the Signatory must go through the in-person issuance process, like they did when the certificate was first issued. Following these practices, if less than 5 years have passed at the time of renewing the certificate, the holder does not need to be physically present for renewal.

Following these practices, if any of the Signatory's or key holder's details have changed, a new registration and issuance process must be carried out, in accordance with the provisions of the relevant sections of this document.

The OSCEPA always issues new keys when certificates are renewed. Therefore, the technical issuance process is the same as when a new request is made.

The OSCEPA gives the Signatory four warnings (30 days, 15 days, 7 days and 1 day before) via email when the certificate is about to expire.

The renewal process can be initiated through the expiry warning email or directly on the OSCEPA website: https://www.signaturaelectronica.ad

This process requires the valid certificate the Signatory wishes to renew.

- Once they have been identified through the certificate to be renewed, the application presents the Signatory with the details from the old certificate and asks them to confirm that they are still valid. The application allows the Signatory to modify the email address associated with the certificate. If other details on the certificate have changed, the certificate must be revoked and a new one must be requested.
- This request process is incorporated into the RA application, where, after reviewing the details, the operator proceeds to request the issuance of a new certificate from the CA.
- As a general rule, the OSCEPA issues a new certificate with a start date that corresponds to the end date of the old certificate. In some cases, in issuance processes through web services, the certificate is renewed with a start date corresponding to the renewal date, before the old certificate is revoked.

4.6.4. New issuance notification to the Subscriber

Notification of the issuance of a renewed certificate will be provided as described in section 4.3.2 of this document.

4.6.5. Conduct that constitutes acceptance of the renewal certificate

See section 4.4.1 of this document.

4.6.6. Publication of renewal certificate by the CA

See section 4.4.2 of this document.

4.6.7. Certificate issuing notification from CA to other entities

In some cases, end entity certificates are sent to the national supervisors that regulate certification authorities' activities.

OCSP certificates are communicated to various government bodies with a certificate validation platform.

Root Certification Authority and Intermediate Certification Authority certificates are signalled to the national supervisor, so that they can be incorporated into its TSL. They are also incorporated into an information repository managed by Mozilla, which includes information on Certification Authorities (CCADB). This database is used by various commercial programmes for the management of their trusted storage providers.

4.7. Certificate re-key

This is the OSCEPA's usual procedure for renewing certificates; therefore, all processes described in section 4.6 refer to this renewal method.

The OSCEPA does not allow certificates to be renewed without being re-keyed.

4.7.1. Circumstances for certificate re-key

Certificate re-keying will usually take place as part of the renewal of a certificate.

4.7.2. Who can request the certification of a new public key?

According to provisions of 4.6.2

4.7.3. Processing certificate re-keying requests

According to provisions of 4.6.3

4.7.4. New issuance notification to the Subscriber

According to provisions of 4.6.4

4.7.5. Conduct that constitutes acceptance of a re-keyed certificate

According to provisions of 4.6.5

4.7.6. Publication of re-keyed certificate by the CA

According to provisions of 4.6.6

4.7.7. Certificate issuing notification from CA to other entities

According to provisions of 4.6.7

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**

Not applicable.

4.8.2. **Who can request a certificate modification?**

Not applicable.

4.8.3. **Processing certificate modification requests**

Not applicable.

4.8.4. **New certificate issuance notification to the Subscriber**

Not applicable.

4.8.5. **Conduct that constitutes acceptance of the modified certificate**

Not applicable.

4.8.6. **Publication of modified certificate by the CA**

Not applicable.

4.8.7. **Certificate issuing notification from CA to other entities**

Not applicable.

4.9. Revocation and suspension of certificates

A revocation is defined as a change in the status of a certificate due to its loss of validity caused by circumstances other than its expiry.

Meanwhile, a suspension is a revocation with cause for suspension (meaning a specific case of revocation); in other words, the certificate is revoked temporarily until a decision is made regarding the definitive revocation or the activation of the certificate.

The maximum certificate suspension period is 7 days. If the end of this suspension period is reached and the certificate has not been activated, the system automatically revokes the certificate definitively and marks the cause as "not specified".

The termination of the validity of an electronic certificate due to revocation or suspension will affect third parties as soon as the notification of this termination is included in the certification service provider's certificate status service (publication of revoked certificates list or consultation of OCSP service).

The OSCEPA keeps certificates on the revocation list until the end of their validity period. At this point, they are removed from the list of revoked certificates. The OSCEPA will only remove a certificate from the revocation list in either of these two situations:

- Certificate expired
- Certificate suspended then deemed unsuitable for definitive revocation following a review

However, the OSCEPA will keep information on the status of an expired certificate in its database, which is accessible through the OCSP service.

Following these practices, under no circumstances shall a revoked certificate be used.

The OCSP response for an expired revoked certificate retains the "revoked" status and the cause.

Due to the different natures of the OCSP and CRL services, should different responses be obtained for an expired certificate, the valid response will be the one offered by OCSP.

For the OSCEPA, the main certificate status consultation service is the one offered by OCSP.

4.9.1. **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 suspension of the digital certificate for a period longer than the one established in this CPS.
- 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.

4.9.2. **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.

4.9.3. **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.

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

Both the revocation management service and the consultation service are considered critical services and therefore appear in the OSCEPA's contingency plan and business continuity plan. These services are available 24 hours a day, 7 days a week. In the event of a system failure, or any other circumstance outside the OSCEPA's control, the OSCEPA will make every effort to ensure that these services are inaccessible for no more than 24 hours.

4.9.4. **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.

4.9.5. **Deadline for CA to process the revocation request**

The OSCEPA will process a revocation request immediately starting from the procedure described in point 4.9.3,

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.

4.9.6. **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.

4.9.7. **Frequency with which CRLs are issued**

CA	Frequency issued	Duration
Andorran Public Administration Certification Entity	24 hours	48 hours

4.9.8. **Maximum latency for CRLs**

CRLs are published every 24 hours and are valid for 48 hours.

4.9.9. **Availability of online revocation check**

The CA provides an online revocation check service via HTTPS at: https://www.camerfirma.com/area-de-usuario/consulta-de-certificados/

And through OCSP consultations at: https://www.signaturaelectronica.ad/consulta-l-estat-del-certificat-ocsp

The access addresses for these services are referenced in the digital certificate. (For CRLs and ARLs, at the CRL Distribution point extension, and the OCSP address, at the Authority Information Access extension).

On certificates, more than one CRL access address may appear to guarantee availability.

The OCSP service is powered by the CRLs issued by the various Certification Authorities (CA) or by access to the platform's (EE) database. Technical access data and OCSP response validation certificates are published on the OSCEPA's website: https://www.signaturaelectronica.ad/consulta-l-estat- del-certificat-ocsp

These services are available 24 hours a day, 7 days a week, 365 days a year.

The OSCEPA will go to every effort to guarantee that the service is never inaccessible for more than 24 consecutive hours, as this is one of the OSCEPA's critical services and is therefore treated as such in its contingency plan and business continuity plan.

The latency for the publication of a revocation on the OCSP service is 1 hour.

4.9.10. Requirements for online revocation check

To check a revocation, the Relying Party must know the email address associated with the certificate they wish to consult, if the check takes place online, or the series number, if the check takes place via the OCSP service.

OCSP responses are signed by the CA that issued the certificate in question; the certificate is therefore needed for the response to be validated. Updated certificates can be found at this link: https://www.signaturaelectronica.ad/consulta-l-estat-del-certificat-ocsp

4.9.11. Other available ways to find out revocation information

The mechanisms the OSCEPA offers system users are published on its website: https://www.camerfirma.com/area-de-usuario/consulta-de- certificados/

4.9.12. Special requirements for revocation due to compromised keys

Not stipulated

4.9.13. Circumstances for suspension

When a suspension takes place, the OSCEPA has a week to decide the certificate's definitive status: (revoked or active). If the OSCEPA does not obtain all the information needed to verify its definitive status in this time, the certificate will be revoked.

If a certificate is suspended, an email will be sent to the Signatory/Subscriber indicating the time of suspension and the cause.

If, after all, the suspension does not lead to a definitive revocation and the certificate must be reactivated, the Signatory/Subscriber will receive an email indicating the certificate's new status.

The suspension process does not apply to:

- AR operator certificates
- OCSP certificates

4.9.14. Who can request a suspension?

See section 4.9.2

4.9.15. Suspension request procedure

The suspension request will be carried out either via access to the relevant page on the OSCEPA website or through previously authenticated written or oral communication. for the Company Stamp the Subscriber must have the revocation code to request suspension of the certificate.

4.9.16. Suspension period limits

Certificates will never be suspended for more than 7 days.

Through an alert system on the certificate management platform, the OSCEPA will ensure that the suspension period established by this CPS is not exceeded.

4.10. Certificate status checking services

4.10.1. Operational characteristics

The OSCEPA offers an issued certificate and revocation list consultation service. These services are available publicly on its website: https://www.camerfirma.com/area-de-usuario/consulta-de-certificados/

4.10.2. Service availability

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

4.10.3. Optional characteristics

Not stipulated.

4.11. 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.

4.12. Key escrow and recovery

4.12.1. Key escrow and recovery policy and practices

Users' keys are generated and stored on a qualified signature creation device; therefore, the certification service provider will never be able to recover any User's key. Should a certificate be lost, it will be revoked and a new one will be issued with a new key pair.

4.12.2. Session key encapsulation and recovery policy and practices

Not stipulated.

5. PHYSICAL, MANAGEMENT AND OPERATIONAL CONTROLS

5.1. Physical security controls

The OSCEPA is subject to annual checks of its compliance with the UNE-ISO/IEC 27001:2007 standard, which regulates the establishment of the appropriate processes for properly managing security on information systems.

The OSCEPA has established physical and environmental security controls to protect resources in the premises where systems, own systems and equipment used for operations are found.

The physical and environmental security policy applicable to certificate generation services offers protection against:

- Unauthorised physical access
- Natural disasters
- Fires
- Support system failure (electrical energy, telecommunications, etc.)
- Collapse of structure
- Floods
- Theft
- Unauthorised exit of equipment, information, media and applications relating to components used for the Certification Service Provider's services

The premises are equipped with preventive and corrective maintenance systems, with 24/7 assistance within 24 hours of notification.

5.1.1. Location and construction

The premises where the OSCEPA is located are built with materials that guarantee protection against attacks through brute force and are found in an easily accessed area at low risk of disaster.

Specifically, the room where cryptographic operations are carried out is a Faraday cage with protection against external radiation, a double floor, fire detection and extinguishing devices, anti-moisture systems, a double refrigeration system and a double electricity supply system.

5.1.2. Physical access

Physical access to the rooms in the premises where the OSCEPA carries out certification processes is restricted and protected through a combination of physical and procedural measures.

It is limited to expressly authorised personnel, with identification at the time of access and records kept of all access, including filming via closed circuit television and archival of this footage.

Any external person must be accompanied by a responsible person from the organisation when entering restricted areas for any reason.

The facilities are equipped with presence sensors at all vulnerable points, as well as with alarm systems that detect intruders and send notifications via other channels.

Rooms are accessed via an ID card reader and managed by an information system that keeps an automatic audit record of entries and exits.

Rooms are accessed via an ID card reader and managed by an information system that keeps an automatic log of entries and exits.

Access to certification systems is protected by 4 levels of access clearance: Building, Offices, CPD and Cryptographic room.

5.1.3. Electricity supply and air conditioning

The premises where the OSCEPA is located are equipped with current stabiliser equipment and a duplicate electrical equipment supply system with engine-generator.

The rooms that house computer equipment are equipped with temperature control systems, with duplicate air conditioning equipment.

5.1.4. Exposure to water

The premises where the OSCEPA is located are situated on a first floor in an area at low risk of flooding. The rooms that house computer equipment are equipped with a moisture detection system.

5.1.5. Fire prevention and protection

The rooms that house computer equipment are equipped with automatic fire detection and extinguishing systems.

Cryptographic devices and media that store keys from Certification Entities have their own specific, additional fire protection system.

5.1.6. Storage system

All removable storage media (tapes, cartridges, CDs, disks, etc.) are only accessible by authorised personnel.

Regardless of the storage device, information classed as confidential is kept in fireproof cabinets or locked cabinets permanently.

5.1.7. Waste disposal

When it is no longer useful, sensitive information is destroyed in the most appropriate way according to the medium on which it is stored.

Print-outs and paper: via shredders or in bins provided specifically before their subsequent controlled destruction.

Storage devices: before being thrown out or reused, they must be processed to be emptied or physically destroyed or the information they contain must be made illegible.

5.1.8. Off-site backup

The OSCEPA uses secure external storage to keep documents and magnetic and electronic devices that are separate from the centre of operations.

At least two expressly authorised people are required to access, deposit or remove devices.

5.2. Procedural controls

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
OSCEPA guarantees at least two people for tasks classed as sensitive. This mainly applies to the handling of the Certification Authority's key storage device.

5.2.3. Identification and authentication for each role
The people assigned for each role are identified by the internal auditor, who will ensure that each of them carries out the operations assigned to them.

Each person only uses the assets needed for their role, thus guaranteeing that no one accesses resources not assigned to them.

Depending on the asset, access to resources is achieved via cryptographic cards or activation codes.

5.2.4. Roles that require separation of duties
Separation of roles table.

	Security officer	System administrat	System operator	CA platform	SSL validation	RA operator
Security officer		Y	N	Y	YES	Y
System administrator	N		N	N	NO	NO
System operator	N	N		N	NO	NO
CA platform auditor	N	N	N		YES	Y
SSL validation specialist	N	N	N	Y		YES
RA operator	N	N	N	N	YES	

5.2.5. Starting and stopping the PKI management system
The PKI system is made up of the following modules:

RA management module, for which the specific page manager services will be activated or deactivated.

Application management module, for which the specific page manager services will be activated or deactivated.

Key management module, located on the HSM device. Can be physically turned on or off.

Database module, centralised management of managed certificates and CRLs, OCSP and TSA. Specific database manager service can be started or stopped.

OCSP module. Online certificate status response server. The system service that deals with this task can be started or stopped.

The module shut-down process follows this sequence:

- Application module
- RA module
- OCSP module
- Database module
- Key management module.

The start-up process follows the same sequence backwards.

5.3. Personnel controls

5.3.1. Qualifications, experience and clearance requirements
All personnel are qualified and have been trained appropriately to carry out 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

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

The personnel who carry out trusted tasks are trained under the terms established by the Certification Policies. There is a training plan that is part of the UNE-ISO/IEC 27001:2007 regulations.

The training includes the following content:

- Security principles and mechanisms in the public certification hierarchy.
- Versions of hardware and applications in use.
- Tasks the person must carry out.
- Management and processing of security incidents and compromises.
- Business continuity and emergency procedures.
- Management and security procedures relating to the processing of personal data.

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

Not stipulated

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

The OSCEPA is subject to annual checks of its compliance with standard UNE-ISO/IEC 27001:2007, which regulates the establishment of the appropriate processes for properly managing security on information systems.

5.4.1. **Types of event recorded**

The OSCEPA records and saves audit logs of all events relating to the CA's security system.

The following events will be recorded:

- System on or off.
- Attempts to create, delete or set passwords or change privileges.
- Attempts to log in or out.
- Unauthorised attempts to access the CA system through the internet.
- Unauthorised attempts to access the archive system.
- Physical access to audit records.
- Changes to the configuration and maintenance of the system.
- CA application records.
- CA application on or off.
- Changes to CA details and/or its keys.
- Changes to the creation of certificate policies.
- Generation of own keys.
- Creation and revocation of certificates.
- Records of the destruction of media that contain keys, activation data, etc.
- Events relating to the life cycle of the cryptographic module, such as reception, use and uninstallation.

The OSCEPA also keeps the following information, either manually or electronically:

- The key generation ceremony and key management databases.
- Physical access records.
- Maintenance and changes to the system configuration.
- Changes to personnel.
- Reports on compromises and discrepancies.
- Records of the destruction of material that contains information on keys, activation data or personal information belonging to the Signatory, in the case of individual certificates, or to the key holder, in the case of organisation certificates.
- Possession of activation data, for operations with the Certification Entity private key.
- Comprehensive reports on any attempts at physical intrusion and vulnerabilities in the infrastructures that support the issuance and management of certificates.

The OSCEPA runs a system that guarantees:

- Enough space to store audit logs.
- No overwriting of audit log files.
-
- That the information saved includes at least: the type of event, date and time, the User carrying out the event and the result of the operation.
- Audit log files will be saved in structured files that may be incorporated into a database to be explored later.

5.4.2. **Frequency with which audit logs are processed**

The OSCEPA reviews its audit logs when a system alert occurs due to an incident.

The processing of the audit logs consists of a review of the logs, which includes verification that they have not been manipulated, a brief inspection of all the log entries and a more in-depth investigation of any alert or irregularity in the logs. All actions taken from the audit review are documented.

5.4.3. **Retention period for audit logs**

The OSCEPA stores audit log information for at least five years.

5.4.4. **Protection of audit logs**

System audit logs are protected from manipulation through a signature on the files that contain them.

They are stored in locked devices and in properly protected repositories.

Their availability is safeguarded as they are stored at facilities outside the centre where the CA is located.

Access to audit log files is reserved exclusively for authorised personnel. The devices are handled by authorised personnel at all times.

There is an internal procedure that details the management processes for devices that contain audit log data.

5.4.5. Audit log backup procedures

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

When the audit log accumulation system records an event, there is no need to send a notification to the individual, organisation, device or application that caused the event.

Notification of whether the result of their action is successful or not can be sent, but not information on whether or not the action has been audited.

5.4.8. Vulnerability analysis

Vulnerability analysis is covered by the OSCEPA's audit processes. Risk and vulnerability management processes are reviewed annually, within the review framework of the UNE-ISO/IEC 27001 standard.

System audit data is stored to be used in the investigation of any incident and to locate vulnerabilities.

The Department of Information Systems carries out an OSCEPA system analysis monthly in order to detect suspicious activity. This report is written up by an external company and includes:

- Intrusion detection - IDS (HIDS).
- OSSEC integrity check system.
- SPLUNK. Operational intelligence.
- Event correlation report.

The OSCEPA corrects any problems reported, which are then recorded by the systems department.

5.5. Record archival

5.5.1. Type of records archived

The following documents involved in the certificate life cycle are stored by the CA or by the RAs:

- All system audit data. PKI and OCSP, incorporating signing events carried out.
- All data relating to certificates, including contracts with the Signatories and the RA. Data relating to identification and location.
- Certificate issuance and revocation requests.
-
- Type of document presented for the certificate application.
- Identity of the Registration Entity accepting the certificate application.
- Unique identification number provided on the previous document.
- All issued or published certificates.
- Issued CRLs or generated certificate status records.
- History of generated keys.
- Communications between PKI elements.
- Certification policies and practices.

The OSCEPA is responsible for archiving all of this material correctly.

5.5.2. Archive retention period

Certificates, contracts with the Subjects/Signatories and any information relating to the identification/authentication of the Subject/Signatory will be retained for at least fifteen years.

Old versions of the documentation will be also preserved for a period of fifteen years by the OSCEPA and may be consulted by interested parties who provide a reason for the consultation.

5.5.3. Archive protection

The OSCEPA ensures the protection of the archives by assigning qualified personnel to process and store them in locked security boxes and off-site facilities.

5.5.4. Archive backup procedures

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

Records are dated with a reliable source via NTP, GPS and radio synchronisation systems.

The OSCEPA has a computer security document that describes the configuration of the time and date parameters on the equipment used to issue certificates.

5.5.6. Audit information collection system

The OSCEPA has a centralised collection system for information on the activities carried out by the equipment involved in the certificate management service.

5.5.7. Procedures for obtaining and verifying archived information

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

5.6. Key changeover

Changing over end entity keys is carried out via a new issuance process (see the corresponding section of this CPS).

Before the CA certificate expires, a key changeover will take place. The CA certificate to be updated and its private key will only be used for signing CRLs while there are still active certificates issued by the aforementioned CA. A new CA certificate will be generated with a new private key and a CN (common name) that differs from the name of the CA certificate to be substituted.

Changes to CA certificates may also be made when the latest developments in cryptography technology (algorithms, key size, etc.) require them to be made.

5.7. Recovery in event of compromised key or disaster

A compromised root key is considered a special case within the contingency and business continuity document. In the event of the substitution of the keys, this incident affects recognition by various applications in the private and public sectors. The recovery of these keys' effectiveness in terms of business will mainly depend on how long these recognition processes take. The contingency and business continuity document incorporates these purely technical and operational terms so that new keys may be available but not recognised by third parties.

The compromise of the algorithms or associated parameters used in the generation of digital certificates or associated services is also included in the contingency and business continuity plan.

5.7.1. Compromised key or incident management procedures

The OSCEPA has developed a contingency plan to recover its critical systems, should an alternative data centre be necessary as part of the UNE-ISO/IEC 27001:2007 certification.

5.7.2. Corruption of resources, applications or data

If a piece of equipment is damaged or stops working but the private keys are not destroyed, the operation must be reset as quickly as possible, prioritising the generation of information on the certificate's status, in accordance with the OSCEPA disaster recovery plan.

5.7.3. Entity's private key compromised

The OSCEPA's contingency plan defined in the UNE-ISO/IEC 27001:2007 certification deems a CA private key compromise a disaster.

In the event of a compromised root key:

- The entity will notify all Signatories/Subscribers, Relying Parties and other CAs with which it has agreements or another type of relationship of the compromise.
- It will indicate that certificates and information regarding the revocation status signed using this key are not valid.

5.7.4. Business continuity following a disaster

The OSCEPA will restore critical services (revocation and publication of revoked certificates) in accordance with the contingency and business continuity plan defined in the UNE-ISO/IEC 27001:2007 certification, with indication of the restoration in the following 24 hours.

The OSCEPA has an alternative centre, which, if necessary, can implement certification systems, as described in the business continuity plan.

5.8. Termination of CA or RA

Before terminating activity, the OSCEPA will take the following action:

- Provide the funds necessary (through a civil liability insurance policy) to finish off its revocation activities.
- Notify all Signatories/Subscribers, Relying Parties and other CAs with which it has agreements or another type of relationship of the termination, at least six months in advance.
- Revoke all authorisation for subcontracted entities to act on behalf of the CA in the certificate issuance procedure.
- Transfer its obligations regarding the maintenance of information in records and logs within a time frame indicated to Subscribers and Users.
- The CA private keys will be destroyed or disabled for future use.
- The OSCEPA will keep active certificates and the verification and revocation system until all issued certificates cease to be valid.

6. TECHNICAL SECURITY CONTROLS

6.1. Key pair generation and installation

6.1.1. **Key pair generation**

The equipment used by the OSCEPA is nCipher. These devices will host root keys and are certified level 3 FIPS 140-2 compliant.

The root keys are generated and managed on an offline device in a cryptographic room.

Intermediate certification authority keys are created on HSM devices, where they are hosted for use. The certificate issued by the root key is created in a secure cryptographic room.

6.1.1.1. Key pair generation by Subscriber

The Subject/Signatory's keys may be created by the Subject/Signatory through hardware (SSCD) or software devices authorised by the OSCEPA, or they may be created by the OSCEPA in PKCS#12 software format.

The STATUS management platform uses its own resources to generate a random robust password and a private key protected by the aforementioned password using the 3DES algorithm. This private key is then used to generate a certificate signature request in PKCS#10 format. With this request, the CA signs the Signatory's certificate. The certificate is delivered to the User in a PKCS#12 file that includes the certificate itself and the private key associated with it. The password for the private key and the PKCS#12 file is never visible on the system.

The keys are generated using the RSA public key algorithm.

Keys may also be created on a remote system through the Web Services layer, which generates a PKCS#10 request and collects the corresponding PKCS#7.

Keys are at least 2048 bits long.

6.1.1.2. Key generation software/hardware

The Signatory/Subscriber's keys may be generated by the Signatory/Subscriber on a device authorised by the OSCEPA. See 6.1.1.1

For intermediate certification authority keys, a cryptographic device that complies with level 2 and level 3 FIPS 140-20 specifications is used.

6.1.2. **Delivery of private key to Subscriber**

See 3.2.1

6.1.3. **Delivery of public key to certificate issuer**

When required by the circuit, the public key may be sent to the OSCEPA in a standard format, preferably PKCS#10, for the certificate to be generated.

6.1.4. **Delivery of public key from CA to Relying Parties**

The CA certificate and its fingerprint will be made available to Users on the following web page: https://www.signaturaelectronica.ad/descarrega-claus-publiques

6.1.5. **Size of keys**

Signatory/Subscriber private keys are based on the RSA algorithm, with a minimum length of 2048 bits,

The period for which the public and private keys can be used varies according to the type of certificate. See section 6.1.1.

6.1.6. **Public key generation parameters and quality assurance**

The intermediate certification authority and Subscriber certificate public key is codified in accordance with RFC 3280 and PKCS#1. The key generation algorithm is RSA

- Size of keys = minimum 2048 bits
- Key generation algorithm: rsagen1
- Encoding method: emsa-pkcs1-v1_5
- Cryptographic hash functions: SHA-256

6.1.7. **Purpose of the use of keys**

All certificates issued contain the "Key Usage" and "Extended Key Usage" attributes, as defined in the X.509v3 standard. More information available in section 7.1.2.

6.2. Protection of private key and standards for cryptographic modules

6.2.1. Controls and standards for cryptographic modules

6.2.1.3. CA private key

The intermediate certification authority signature private key is maintained on a cryptographic device that complies with level 3 FIPS 140-2 specifications.

When the CA private key is outside of the device, it is encrypted.

A backup of the CA signature private key may be stored and recovered only by authorised personnel in accordance with the trusted roles, using at least a dual control on a secure physical medium.

Backup copies of the CA signature private key are stored securely. This procedure is described in detail in the OSCEPA's security policies.

6.2.1.4. Subscriber's private key

The Subscriber's private key may be stored on a software or hardware device,

When it is stored in software format, the OSCEPA will provide the appropriate configuration instructions for secure use.

All cryptographic devices distributed by the OSCEPA to host qualified certificates comply with all qualified signature creation device requirements and are therefore suitable for qualified signature creation.

Information regarding the key creation and storage process used by the OSCEPA is included in the digital certificate itself, through the corresponding OID, so that the User can act accordingly.

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

Multi-person control is required to activate the CA private key. In the case of this CPS, the policy is 2 to 4 people for key activation.

6.2.3. Private key escrow

The OSCEPA does not store or copy holders' private keys. Exceptions:

- In the case of certificates for information encryption, the OSCEPA can keep a copy of the key.

6.2.4. Private key backup

The OSCEPA makes a backup copy of CA private keys so that they can be recovered in the event of a disaster, loss or damage. Both the generation of this copy and its recovery require the participation of at least two people.

These recovery files are stored in fireproof cabinets and in the off-site storage centre.

Signatory keys held on software may be stored to be recovered, in the event of a contingency, on an external storage device separate to the installation key, as indicated in the software key installation manual.

Signatory keys held on hardware cannot be copied, as they cannot leave the cryptographic device.

The OSCEPA keeps records of all CA private key management processes.

6.2.5. Private key archival

CA private keys are archived for 10 years counting from the issuance of the last certificate. They will be stored in secure fireproof archives and in the external storage centre. At least two people will be required to recover the CA private key on the initial cryptographic device.

The Signatory may store the keys delivered via software for the duration of the certificate's validity; after this, they must destroy them, ensuring that they do not have any information encrypted by the public key.

Only in the case of encryption certificates shall the Signatory be able to store the private key for however long they deem necessary. In this case, the OSCEPA could also save a copy of the private key associated with the encryption certificate.

When their certificate is delivered, for three working days, the OSCEPA will provide holders of certificates that come with a private key generated by the service provider with a downloadable PKCS#12 file, which contains the private key and its associated certificate.

The OSCEPA keeps records of all CA private key management processes.

6.2.6. Entering the private key in the cryptographic module

Intermediate certification authority keys are stored in online network HSM equipment, so that they may be accessed from PKI applications for certificate generation.

6.2.7. Storing the private key in the cryptographic module

Intermediate certification authority keys are stored in online network HSM equipment, so that they may be accessed from PKI applications for certificate generation.

6.2.8. Private key activation method

The Subscriber's private key can be accessed through an activation key known only by the Subscriber, who will avoid writing it down.

The activation of the intermediate certification authority's private key is managed by the HSM management application.

The OSCEPA keeps records of all CA private key management processes.

6.2.9. Private key deactivation method

When the key is held in software format, it may be deactivated through the deletion of the relevant keys from the corresponding application on which they are installed.

To deactivate the CA private key, the steps detailed in the administrator's manual for the corresponding cryptographic equipment must be followed.

For CA keys, a cryptographic ceremony will take place and be recorded.

6.2.10. Private key destruction method

Prior to the destruction of the keys, a revocation for the public key certificate associated with the private keys will be issued.

The devices storing any part of the CA private keys will be physically destroyed or will undergo low-level formatting. To get rid of them, the steps detailed in the administrator's manual for the cryptographic equipment must be followed.

Finally, security backups will be destroyed securely.

Subscriber keys held on software may be destroyed through deletion, in accordance with the instructions for the application housing them.

Subscriber keys held on hardware may be destroyed through special software at registration points or the CA.

The OSCEPA keeps records of all CA private key management processes.

6.2.11. Cryptographic module capabilities

The cryptographic modules are certified level 3 FIPS-140-2 and are handled by at least two operators in an HSM model. All equipment is housed in a secure environment. The cryptographic model that stores root keys is managed within an isolated, disconnected cryptographic room. Cryptographic modules that store intermediate certification authority keys are stored in secure environments within a CPD, in accordance with the ISO-27001 standard.

6.3. Other aspects of key pair management

6.3.1. Public key archival

In accordance with the provisions of article 26 of Andorran Law 35/2014, of 27 November, on electronic trust services, archives will be kept for a period of

at least fifteen (15) years, as far as technology allows this. Documents to be stored include the public key certificates issued to the Subscribers and own public key certificates.

6.3.2. Period of use for public and private keys

The private key must not be used after the validity period for the associated public key certificate.

The public key or its certificate may be used as a verification mechanism for data encrypted by the public key outside this time frame for validation purposes.

A private key may only be used outside the period established by the corresponding digital certificate to recover encrypted data.

6.4. Activation data

6.4.1. Generation and activation of activation data

User private key activation data is generated in different ways depending on the type of certificate.

In software. The certificate is generated by the service provider and delivered in a standardised PKCS#12 file protected by a password generated by the management application and delivered to the Subject through the email address associated with the digital certificate.

On hardware device. The cards used by the OSCEPA are generated at the registration point and are protected by a PIN and a PUK calculated at the factory. This information is sent via the management platform to the Subject through the email address associated with the digital certificate. The Subject has access to software that can change their card's PIN and PUK.

On a third-party hardware device (HSM). The OSCEPA recognises some third-party devices, even though they are managed independently. The keys are generated in a separate ceremony, then a certificate issuance application and ceremony records are delivered to the OSCEPA.

6.4.2. Protection of activation data

Activation data is communicated to the Subject via a channel separate to the PKI management platform. The OSCEPA does not store this information in its database in the case of software- or hardware-format certificates. They are not stored on the centralised platform, as they are known and held by the holder. Data may be resent to the Subject upon request to the address associated with the certificate, and will be effective for as long as the User does not make a change to it.

6.4.3. Other aspects of activation data

Not stipulated.

6.5. Computer security controls

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:

1. Operating system's security configuration.
2. Applications' security configuration.
3. Correct system sizing.
4. Configuration of Users and permissions.
5. Configuration of log events.
6. Backup and recovery plan.
7. Antivirus configuration
8. Network traffic requirements

6.5.1. Specific computer security technical requirements

Each OSCEPA server includes the following functionalities:

- control of access to CA services and privilege management
- enforcement of separation of tasks for privilege management
- identification and authentication of roles associated with identities
- archival of Subscriber and CA history and audit data
- audit of security events
- security self-diagnosis relating to CA services
- CA system and key recovery mechanisms

The functionalities detailed here are achieved through a combination of operating system, PKI software, physical protection and procedures.

6.5.2. Assessment of computer security

The security of the equipment is reflected in an initial risk analysis. Therefore, the security measures implemented are a response to the probability and impact of a group of threats making the most of security breaches.

6.6. Life cycle security controls

When the cryptographic keys associated with a certificate are stored on a hardware device, this is guaranteed to be a qualified signature creation device that fulfils appendix II of eIDAS. The hardware device may be a cryptographic card, USB token or HSM.

About hardware devices:

a) Hardware devices are prepared and stamped by an external provider.
b) Distribution of this medium is managed by the external provider, who distributes it to the Registration Authorities to be delivered to the Signatory.
c) The Signatory or the RA uses the device to generate the key pair and send the public key to the CA.
d) The CA sends a public key certificate to the Signatory or to the RA, which is then entered into the device.
e) The device is reusable and can hold several key pairs securely.
f) The device is kept by the Subject/Signatory.

About the devices used on the centralised key management platform: The device that stores these keys is certified level 3 FIPS-104-2 or EAL4 and approved by the European supervisor for services catalogued as QSCDManagedOnBehalf.

6.6.1. System development controls

The OSCEPA has implemented a procedure to track the changes in versions of operating systems and applications that imply an improvement to their security functions or that correct any vulnerability detected.

As a response to the intrusion and vulnerability analyses, adaptations are made to the systems and applications that may present security problems, while in response to the security alerts received from the managed security services subcontracted to third parties, the corresponding RFC (Requests for Changes) are executed to incorporate the security patches or updates to the problematic versions.

The RFC incorporates and documents measures taken for the approval, execution or refusal of these changes.

In cases where the execution of an update or correction of a problem involves a situation of vulnerability or a significant risk, this is incorporated into the risk analysis and alternative controls are carried out until the risk level is manageable.

6.6.2. Security management controls

6.6.2.1. 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.

6.6.2.2. 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.

6.6.2.3. 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.

6.6.2.4. 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

a) There are controls based on firewalls, antivirus and high-availability IDS.
b) Sensitive data is protected by cryptographic techniques or access controls with strong authentication.
c) The OSCEPA has documented its user registration and termination procedure and detailed access policy in its security policy.
d) The OSCEPA implements the procedures needed to guarantee that operations are carried out in accordance with the roles policy.
e) Each person is associated with a role to carry out certification operations.
f) 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.

6.6.2.5. 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

Not stipulated

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

The OSCEPA has a time synchronisation procedure coordinated with the ROA (the Royal Spanish Navy Institute and Observatory) in San Fernando via NTP. It also uses GPS and radio synchronisation as secure sources.

7. CERTIFICATE, CRL AND OCSP PROFILES

7.1. Certificate profile

Certificate profiles comply with RFC 5280.

All qualified or recognised certificates issued under this policy comply with version 3 of the X.509 standard and with the RFC 3739 and ETSI 101 867 "Qualified Certificate Profile" standards.

The profiles for these certificates may be requested at gestion_soporte@camerfirma.com or on +34 902 361 207

7.1.1. **Version number**

OSCEPA issues X.509 Version 3 certificates.

7.1.2. **Certificate extensions**

The certificate extension documents are detailed on the profile pages. The profiles for these certificates may be requested at gestion_soporte@camerfirma.com or on +34 902 361 207

7.1.3. **Algorithm object identifiers (OID)**

The signature algorithm object identifier is

- 1.2.840.113549.1.1.5 - sha1withRSAEncryption
- 1.2.840.113549.1.1.11 - sha256WithRSAEncryption

The *Subject Public Key Info* field (1.2.840.113549.1.1.1) includes the value *rsaEncryption*

7.1.4. **Name format**

Certificates must contain the information needed for them to be used, as defined by the corresponding authentication, electronic signature, encryption or electronic evidence policy.

In general, certificates used in the public sector must detail the identity of the person receiving the certificate, preferably in the Subject Name or Subject Alternative Name fields, including the following details:

- First name and surname of the Signatory, whether they are the holder or a representative, in separate fields, or with indication of the algorithm that separates them automatically.
- The legal person's name, when applicable.
- The corresponding ID document numbers, in accordance with the legislation that applies to the Signatory, whether they are the holder or representative and whether they are a natural or a legal person.

The exact name semantics are described on the profile pages. The profiles for these certificates may be found at https://www.signaturaelectronica.ad/jerarquia-politiques-i-practiques-de-certificacio.

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)**

All Camerfirma certificates have a policy object identifier that starts from the base 1.3.6.1.4.1.17326.

Govern d'Andorra (OSCEPA) = 2.16.20.2.1.3.1

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**

Not stipulated

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

The CRL profile corresponds to the one proposed in the corresponding certification policies. The CRLs are signed by the CA that issued the certificate.

The detailed CRL profile may be requested at https://www.camerfirma.com/ayuda/soporte/ or on +34 902 361 207.

7.2.1. **Version number**

The CRLs issued by the OSCEPA are version 2.

7.2.2. **CRL and extensions**

These are imposed by the corresponding certification policies. The detailed profile of CRL and its extensions may be requested at https://www.camerfirma.com/ayuda/soporte/ or on +34 902 361 207.

7.3. OCSP profile

7.3.1. **Version number**

OCSP responder certificates are version 3. These certificates are issued by the CA managed by the OSCEPA, in accordance with the RFC 6960 standard.

7.3.2. **OCSP extensions**

The profile of the OCSP responder certificates may be obtained at the following email address gestion_soporte@camerfirma.com or by telephone on +34 902 361 207.

An up-to-date list of OCSP certificates may be obtained at

8. COMPLIANCE AUDITS

The OSCEPA is committed to security and service quality.

The OSCEPA's aims in terms of security and quality have mainly been the achievement of ISO/IEC 27001 and ISO/IEC 20000 certification and the execution of two-yearly internal audits to the OSCEPA's certification system and to the Registration Authorities, in order to guarantee compliance with internal procedures.

The OSCEPA is subject to periodic audits with the WEBTRUST for CA stamp, which ensures that its policy documents and CPS have the right format and scope and that they are fully aligned with its certification policies and practices.

The OSCEPA is also subject to activity monitoring carried out by the national regulatory body, which is the National Accreditation Commission (CNAC).

Registration Authorities that belong to both these hierarchies are subject to an internal audit process. These audits are carried out periodically and discretionally based on a risk assessment according to the number of certificates issued and the number of registration operators, which will also determine whether the audit is carried out in person or remotely. Audits are described in an "Annual Audit Plan".

The OSCEPA is subject to a two-yearly data protection audit.

The OSCEPA will carry out an internal audit. In this audit, the OSCEPA will check a handful of certificates issued by a certain Registration Authority at random and ensure that the evidence collected is correct and sufficient for the certificate to be issued.

8.1. Frequency or circumstances of audits

As indicated in prior section, the OSCEPA carries out compliance audits annually, in addition to the internal audits carried out discretionally.

- WEBTRUST for CA: annual.
- Vulnerability analysis: quarterly.
- Intrusion analysis: annual.
- RA audits: discretionally.

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 are carried out by the following external independent companies, which are widely recognised for their expertise in computer security, information system security and Certification Authority compliance audits:

- • For the WebTrust audit: Awarded by public call for tenders

8.3. Relationship between auditor and CA

The audit companies used are independent, their prestige is widely recognised and they have departments specialising in carrying out computer audits in digital certificate and trusted service management; there is therefore no conflict of interests that may distort their activity in relation to the CA.

There is no financial or organic dependency or link between the audit companies and the CA, the OSCEPA.

8.4. Topics covered by audit

In general terms, audits check:

a) That the OSCEPA follows a system that guarantees the quality of the service it provides.
b) That the CPS complies with the provisions of the policies, with the agreements made by the authority that approved the policies and with the provisions of the regulations in force.
c) That the OSCEPA is managing the security of its information systems appropriately.
d) Audits also check that certificates are aligned with the policies set out by the CA/B Forum in its "Baseline Requirements".

In general terms, the elements subject to auditing are as follows:

- Processes carried out by the OSCEPA, RAs and related elements when issuing certificates and providing

OCSP online validation services.
- Information systems.
- The protection of the data processing centre.
- The documentation required for each type of certificate.
- Verification that the RA operators are familiar with the OSCEPA's CPS.

8.5. Action taken as a result of deficiencies

Once the compliance audit report is received, the OSCEPA will discuss the deficiencies found with the entity that carried out the audit before developing and executing a corrective plan in order to remedy these deficiencies.

If the audited entity is unable to develop and/or execute this plan in the required time period, or if the deficiencies found constitute an immediate threat to the system's security or integrity, this must be communicated immediately to the policy authority, which may take the following action:

- Cease operations temporarily.
- Revoke the corresponding certificate and regenerate the infrastructure.
- Terminate the Entity's services.
- Other complementary action deemed necessary.

8.6. Communication of results

The results are communicated to the security and regulatory compliance officer by the auditors who carried out the assessment. This takes place in an event attended by corporate management. The audit certificate is published on the OSCEPA website.

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**

The OSCEPA provides free access to information relating to certificate status or revoked certificate status through a list of revoked certificates or through access online on the OSCEPA website: https://www.signaturaelectronica.ad/consulta- l-estat-del-certificat-ocsp.

The OSCEPA offers the OCSP service for free. https://ocsp.govern.ad.

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**

Not stipulated.

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:

a) That contained in this CPS and in Certification Policies.
b) That contained in certificates.
c) Any information to which accessibility is not prohibited by the regulations in force.
d)

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/suspension of certificates

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

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

The OSCEPA offers an online status consultation service for certificates based on the OCSP standard on the following website: http://ocsp.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. Privacy of personal information

9.4.1. Privacy plan

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. Information treated as private

An individual's personal information that is not publicly available in the content of a certificate or CRL is considered private.

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 or suspension 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 suspension and 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, suspension, 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 suspension/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 suspension or 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

Not stipulated

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 suspension or 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/suspension 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, CA/B Forum, 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

Not stipulated

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.

1. APPENDIX I: document history

Octubre del	V1.0	Versió inicial
Novembre del	V1.0	**Revisió**
Octubre del 2019	V2.0	**Canvi d'ordre, denominació i desenvolupament en diversos punts per alinear-se amb l'RFC3647**
Febrer 2020	V2.1	**Canvi de sintaxis**
Març-Abril 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**