PERSONES NATURALS CERTIFICATE POLICY OF ANDORRAN PUBLIC ADMINISTRATION PKI

Govern d'Andorra

Version 1.0.1

Language: **English**

Table of Contents

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 policies followed by the Office for Electronic Trust Services of the Principality of Andorra – hereinafter OSCEPA – when issuing digital certificates within this infrastructure.

These policies are aligned with the requirements set out in version 1.7.3 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 Persones Naturals Certificate Policies (CP).

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 certificates, which may be identified through the certificate policy object identifier contained in the certificate's certificatePolicy extension. The types of certificates 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 certificates:

- 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.

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 CP 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 CP, the following may act as an RA:

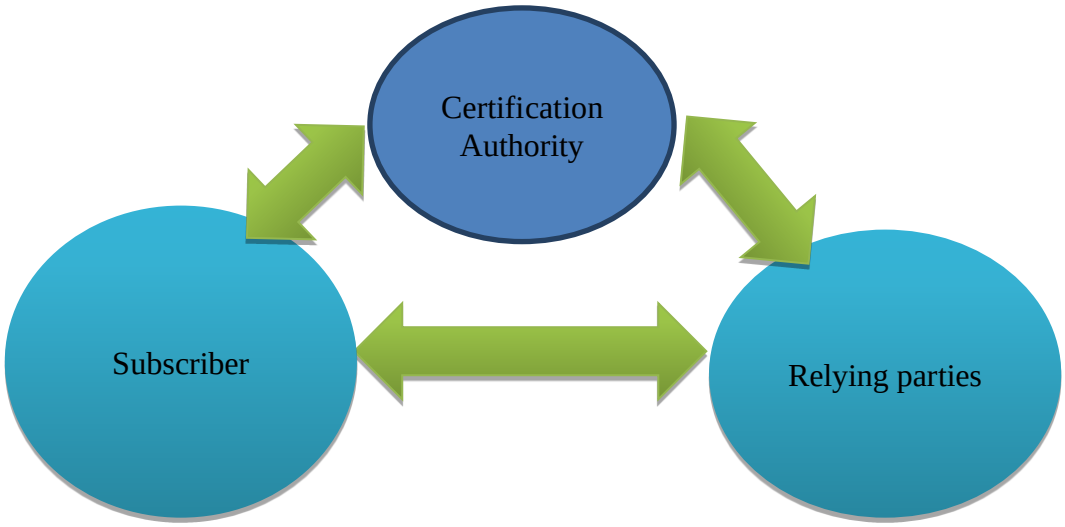
- The Certification Authority itself.
- Any national or international agent that maintains a contractual relationship with the CA and that goes through the registration and audit procedures that demonstrate that it fulfils the requirements set out in this document.

1.3.3 Subscribers

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 parties

In this CP, 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.



1.4. Certificate usage

1.4.1 Appropriate certificate uses

The Certificates of the OSCEPA for Natural Persons can be used for the following purposes:

Identification of the Signatory/Subscriber and/or their link to the entity: The Signatory/Subscriber of the Certificate can authenticate, in front of a Subscriber of the Certificate can authenticate, on the other hand, his or her identity and/or the association of his/her private key with the respective public key, as contained in the certificate.

The Signatory/Subscriber may validly identify him/herself to any person by signing an electronic mail or any other type of data.

Integrity of the signed document: The use of this Certificate guarantees that the signed document is complete, it is signed is complete, that is to say, it guarantees that the document has not been altered or modified after being signed by the Signatory/Subscriber. It certifies that the message received by the Trusting Third Party is the same as the one sent by the Signatory/Subscriber.

Non-repudiation of origin: The use of this Certificate also guarantees that the person signing the document cannot repudiate the document cannot repudiate it, that is to say, the Signatory/Subscriber who has signed it cannot deny the authorship or integrity of the document.

Although it is possible to use it for data encryption, the CA is not responsible for this activity, because, for security reasons, the PC determines that the CA does not keep a copy of the Signatory/Subscriber's private key. There is no guarantee, therefore, of the recovery of the encrypted data in the event of loss of the private key by the Signatory/Subscriber or the Relying Third Party. This use will be made, in any case, under the responsibility of the Signatory/Subscriber.

1.4.2 Prohibited certificate uses

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 the CP and in the CPS.

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 CP, 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 CP, 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 administration

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.

1.5.1 Organization administering the document

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

1.5.2 Contact person

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

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

1.6. Definitions and acronyms

1.6.1 Acronyms

CA	Certification Authority
CPS	Certification Practice Statement.
CRL	Certificate Revocation List. List of revoked certificates
CSR	Certificate Signing Request.
DES	Data Encryption Standard. Standard for encrypting data
DN	Distinguished Name. Distinguished name in the digital certificate
DSA	Digital Signature Algorithm. The signature's algorithm standard
FIPS	Federal Information Processing Standard Publication
IETF	Internet Engineering Task Force
ISO	International Standards Organization
ITU	International Telecommunications Union.
LDAP	Lightweight Directory Access Protocol. Protocol for directory access
OCSP	On-line Certificate Status Protocol. Protocol for accessing the status of certificates
OID	Object Identifier.
PA	Policy Authority.
PC	Certification Policy
PIN	Personal Identification Number.
PKI	Public Key Infrastructure.

RA	Registration Authority
RSA	Rivest-Shamir-Adleman. Type of encryption algorithm
SHA	Secure Hash Algorithm.
SSCD	Secure Signature Creation Device
SSCDSD	Secure Signature Creation Data Storage Device
SSL	Secure Sockets Layer. A protocol designed by Netscape that has become standard on the Internet. It allows the transmission of encrypted information between a browser and a server.
TCP/IP	Transmission Control. *Protocol/Internet Protocol*. System of protocols, as defined in the IETF framework. The TCP protocol is used to split source information into packets and then recompile it on arrival. The IP protocol is responsible for correctly directing the information to the recipient.

1.6.2 Definitions

Activation data	Private data such as PINs or passwords used for activating the private key
Applicant	Within the context of this certification policy, the applicant is a natural person with special powers to carry out certain procedures on behalf of the entity.
Certificate	A file that associates the public key with some data identifying the Subject/Signatory and signed by the CA.
Certification Authority	This is the entity responsible for issuing and managing digital certificates. It acts as the trusted third party between the Subject/Signatory and the User Party, associating a specific public key with a person.
Certification Policy	A set of rules defining the applicability of a certificate in a community and/or in an application, with common security and usage requirements.
CPS	Defined as a set of practices adopted by a Certification Authority for issuing certificates in compliance with a specific certification policy.
CRL	A file containing a list of certificates that have been revoked for a certain period of time and which is signed by the CA.
Cross certification	Establishing a trust relationship between two CAs, by exchanging certificates between the two under similar levels of security.

Digital signature	The result of the transformation of a message, or any type of data, by the private application in conjunction with known algorithms, thus ensuring: a) that the data has not been modified (integrity) b) that the person signing the data is who he/she claims (ID) c) that the person signing the data cannot deny having done so (non-repudiation at origin)
Entity	Within the context of these certification policies, a company or organization of any type with which the applicant has any kind of relationship.
Key pair	A set consisting of a public and private key, both related to each other mathematically.
OID	A unique numeric identifier registered under the ISO standardization and referring to a particular object or object class.
PKI	A set of hardware, software and human resources elements and procedures, etc., that a system is made up of based on the creation and management of public key certificates.
Policy authority	A person or group of people responsible for all decisions relating to the creation, management, maintenance and removal of certification and CPS policies.
Private key	A mathematical value known only to the Subject/Signatory and used for creating a digital signature or decrypting data. Also called signature creation data.
Public key	A publicly known mathematical value used for verifying a digital signature or encrypting data. Also called signature verification data. The CA's private key is to be used for signing certificates and CRLs.
Registration Authority	The entity responsible for managing applications and identification and registration of certificates.
SCDSD	*Secure Signature Creation Data Storage Device* A software or hardware element used to safeguard the Subject/Signatory's private key so that only he/she has control over it.

SSCD	Secure Signature Creation Device. A software or hardware element used by the Subject/Signatory for generating digital signatures, so that cryptographic operations are performed within the device and control is guaranteed solely by the Subject/Signatory.
Subject/Signatory	Within the context of this certification practices statement, the natural person whose public key is certified by the CA and who has a valid private key for generating digital signatures.
User Party	Within the context of this certification policy, the person who voluntarily trusts the digital certificate and uses it as a means for accrediting the authenticity and integrity of the signed document.

2. Publication and Repository Responsibilities

2.1. Repositories

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

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 CP will be governed by the provisions of the corresponding section of the CP.

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

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

The Certificates of the Government of Andorra for Personas Naturals allow the identification of a natural person in the scope of their activity.

The certificates of the Government of Andorra for natural persons within the "Global Chambersign ROOT" hierarchy are as follows:

- Pertinència a entitat.
- Persona física.
- Persona física com a ciutadà Andorrà.
- Persona física professional.
- Persona física com a professional qualificat.
- Empleat públic.
- Representació de persona jurídica.
- Representació de persona física.

Identification and authentication of OSCEPA is described in its CPS.

4. Certificate life-cycle operational requirements

Identification and authentication of OSCEPA is described in its CPS.

5. Facility, management, and operational controls

Facility, management, and operational controls of OSCEPA is described in its CPS.

6. Technical Security Controls

Technical Security Controls of OSCEPA is described in its CPS.

7. Certificate, CRL, and OCSP profiles

7.1. Certificate profile

The certificates issued by the CA meet the requirements of the ITU X.509, RFC 5280 and RFC 6818 standards, as well as ETSI TS 101 867.

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

7.2. CRL profile

The certificate revocation lists issued meet the requirements of ITU X.509, RFC 5280 and RFC 6818 standards.

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

7.3. OCSP profile

This service complies with RFC 6960 standard.

The detailed OCSP profile and the OCSP responder certificates may be requested at https://www.camerfirma.com/ayuda/soporte/ or on +34 902 361 207.

8. Compliance Audit and other Assessments

The compliance audit and other assessments of OSCEPA is described in its CPS.

9. Other Business and Legal Matters

The obligations of the holders of a Government of Andorra Certificate for Natural Persons:

- Provide the CA with the information necessary to carry out a correct identification.
- Make all reasonable efforts to confirm the accuracy and truthfulness of the information provided.
- To safeguard their private key in a diligent manner.
- Inform of the existence of any cause for revocation.
- Notify any change in the data provided for the creation of the certificate during its validity period.
- Not to monitor, manipulate or carry out reverse engineering on the technical implementation of the certification services.

It will be the obligation of the third parties that rely on a Certificate of the Government of Andorra for Natural Persons:

- Verify the validity of the certificates at the moment of carrying out any operation based on the same.
- Know and accept the guarantees, limits, and responsibilities applicable to the acceptance and use of the certificates on which they are relying, and accept to be subject to these guarantees, limits, and responsibilities.
- Limit the reliability of the certificates to the permitted uses of the same, in accordance with the provisions of the certificate extensions and the relevant CP.
- Notify any fact or anomalous situation related to the certificate that could be considered as a cause for revocation of the certificate.

The CA will not be responsible in any case when faced with any of these circumstances:

- State of war, natural disasters, or any other case of force majeure.
- For the use of the certificates as long as it exceeds the provisions of the current regulations and the CP.
- For the improper or fraudulent use of certificates or CRLs issued by the CA.
- For the use of the information contained in the Certificate or in the CRL.
- Failure to comply with the obligations established for the Subscriber or Trusting Third Party in the regulations in force, the CP or the corresponding practices.
- For the damage caused during the period of verification of the causes for revocation.
- Fraud in the information presented by the applicant.

The Government of Andorra does not have a specific reintegration policy and complies with the general regulations in force.

The CA must determine the information to be considered confidential, and in any case must comply with current legislation on data protection and specifically with the provisions of Law 15/2003, of 18 December, on the Protection of Personal Data (LQPDP).

The RA that constitutes the PKI of the Government of Andorra must verify that the applicant for a certificate is informed and gives his or her consent to the processing of his or her personal data, the purpose for which it is to be used, the recipients of the data and its inclusion in the file declared for this purpose by the Government of Andorra.

The owners of the data may exercise their rights of access, rectification, and opposition by writing to the contact address indicated in this document.

The data contained in the Directori de Certificats are considered personal data for the purposes of the provisions of the LQPDP and other complementary legislation, which is why access by third parties is not permitted.

APPENDIX I: document history

2020 January	V1.0.0	Initial version
2021 July	V1.0.1	Annual review