Tinexta Infocert

CERTIFICATE POLICY

FOR PERSONAL CERTIFICATES

(FOR NATURAL PERSON)

CAMERFIRMA

Version 1. 0

Drafting and Review: Camerfirma's Compliance and Legal Departments

Approval (AP): Camerfirma's Legal Department

Document valid only in digital format signed or electronically sealed by the Policy Authority (PA).

This document can be obtained from the address:
https://www.camerfirma.com/practicas-de-certificacion-ac-camerfirma-cps-dpc/

Language: English

Code: PUB-2025-18-12

SELLO JURIDICO

Firmado digitalmente por SELLO JURIDICO
Fecha: 2025.05.29 15:43:43 +02'00'

INDEX

APENDICE 1 HISTORY OF THE DOCUMENT 51

1 INTRODUCTION

1.1 OVERVIEW

The Certification Policy (hereinafter CP) is a document that establishes the requirements, rules and procedures governing the issuance, use, management and revocation of electronic certificates. Its objective is to ensure trust and security in the digital identity of certificate Subjects and in the transactions they perform with their certificate.

Therefore, this CP establishes the requirements, rules and procedures applicable to the issuance, use, management and revocation of personal electronic certificates issued by Camerfirma.

Camerfirma's Certification Practice Statement (hereinafter CPS) contains the basic concepts about electronic certificates, electronic signature, Public Key Infrastructure, etc... so it is recommended to consult the CPS in case you are not familiar with these concepts.

This document is structured according to the IETF RFC 3647 standard.

Under this CP, Camerfirma issues the following types of certificates:

- **Qualified Citizen Certificate**:
  This qualified certificate identifies a natural person (Subject/Signatory) only to act in his/her own name.

  Camerfirma issues these qualified certificates in secure signature creation devices - QSCD (card, cryptographic token or cloud) under OID 0.4.0.194112.1.2 according to ETSI EN 319 411-2 - QCP-n-qscd, and in non-QSCD devices under OID 0.4.0.194112.1.0 according to ETSI EN 319 411-2 - QCP-n.

- **Qualified Corporate / Self-Employed / Chartered Self-Employed Certificate**

  Corporate Qualified Certificate
  This qualified certificate identifies a natural person (Subject/Signatory) and determines, as specific attributes, its relationship (labor, mercantile, collegial, etc.) with an Entity.

  Qualified Certificate for Self-Employed
  This qualified certificate identifies a natural person (Subject/Signatory) and determines, as specific attributes, his/her status as a self-employed person, his/her economic activity and, if applicable, the registered trade name under which the self-employed person carries out his/her profession.

  Qualified Certificate for Chartered Self-Employment
  This qualified certificate identifies a natural person (Subject/Signatory) and determines, as specific attributes, his status as a self-employed person, his economic activity, his status as a registered professional, and if applicable, the registered trade name under which the self-employed person practices his profession.

Camerfirma issues these qualified certificates on QSCD devices (card, cryptographic token or cloud) under OID 0.4.0.194112.1.2 according to ETSI EN 319 411-2 - QCP-n-qscd, and on non-QSCD devices under OID 0.4.0.194112.1.0 according to ETSI EN 319 411-2 - QCP-n.

- **Qualified Certificate for a Legal Representative of a Legal/Non-Legal Entity**

  This qualified certificate identifies a natural person (Subject/Signatory) and determines, as specific attributes, his/her status as a legal representative or representative with full powers, with the capability to act on behalf of a Legal or Non-Legal Entity.

  It is aimed at legal representatives of Legal Entities (Sole Administrator, Joint Administrator,Managing Director, etc.), legal representatives of Non-Legal Entities (Sole Administrator, Joint Administrator, Director/Manager, President of Property Owners, etc.), and representatives with very broad powers of representation of Legal Entities (similar to those of a legal representative)that allows them to act both in the field of the Entity's relations and procedures with the Public Administrations (authentication and signature uses) and in the field of contracting goods or services relating to the ordinary business of the Entity (signature uses).

  The jointly legal representatives and the jointly representatives who want to request this certificate must hold powers that include the joint power to represent the Legal or Non-Legal Entity to carry out relations and procedures with Public Administrations.

  In any case, the certificate Subject is responsible for using it in accordance with its powers and the Relying Party is responsible for verifying its content and scope.

  The certificates issued under these CPs are in accordance with the Spanish national regulations for certificate profiles for a natural person representative of a legal entity and for a natural person representative of a non-legal entity established in section 14.1 of the document "Electronic certificate profiles" of the Sub-directorate General for Information, Documentation and Publications of the Ministry of Finance and Public Administrations., whose OID is 2.16.724.1.3.5.8 for legal representative and OID 2.16.724.1.3.5.9 for legal representative of a Non-Legal entity.

  Camerfirma issues these qualified certificates on QSCD devices (card, cryptographic token or cloud) under OID 0.4.0.194112.1.2 according to ETSI EN 319 411-2 - QCP-n-qscd, and on Non-QSCD devices under OID 0.4.0.194112.1.0 according to ETSI EN 319 411-2 - QCP-n.

- **Qualified Certificate for a Voluntary Representative of a Legal/Non-Legal Entitybefore the Public Administrations**

  This qualified certificate identifies a natural person (Subject/Signatory) and determines, as specificattributes, his/her capability to represent a Legal or Non-Legal Entity in the field of the

Entity's relations and procedures with Public Administrations (authentication and signature uses).

It is aimed at representatives with a general power or a specific power which includes faculties that enable them to perform, on behalf of the Legal or Non-Legal Entity, actions and procedures with Public Administrations that require the use of electronic signature or electronic certificate.

The jointly representatives who want to request this certificate must hold powers that include the joint power to represent the Legal or Non-legal Entity to carry out relations and procedures with Public Administrations. Alternatively, they can provide a specific power or a reliable document signed by all the representatives in favour of one of them.

In any case, the certificate Subject is responsible for using it in accordance with its powers and the Relying Party is responsible for verifying its content and scope.

The certificates issued under these CPs are in accordance with the Spanish national regulations for certificate profiles for a natural person representative of a legal entity and for a natural person representative of a non-legal entity established in section 14.1 of the document "Electronic certificate profiles" of the Sub-directorate General for Information, Documentation and Publications of the Ministry of Finance and Public Administrations. whose OID is 2.16.724.1.3.5.8 for legal representative and OID 2.16.724.1.3.5.9 for legal representative of a Non-Legal entity.

Camerfirma issues these qualified certificates on QSCD devices (card, cryptographic token or cloud) under OID 0.4.0.194112.1.2 according to ETSI EN 319 411-2 - QCP-n-qscd, and on Non-QSCD devices) under OID 0.4.0.194112.1.0 according to ETSI EN 319 411-2 - QCP-n.

- **Qualified Certificate for a Special Representative of a Legal/Non-Legal Entity**

This qualified certificate identifies a natural person (Subject/Signatory) and determines, as specific attributes, its capacity to act on behalf of an Entity with or without legal personality only for certain powers framed in its function or department in the Entity (uses of signature of private documents of the ordinary commercial traffic of the Entity).

This certificate is not valid for authentication or signature uses on behalf of the Entity with or without legal personality in platforms of the Public Administration, due to the implicit limitation of the powers whose exact scope cannot be known by the Relying Party.

The jointly representatives who want to request this certificate must hold powers that include the corresponding powers framed in his/her function/department in the Entity. Alternatively, they can provide a specific power or a reliable document signed by all the representatives in favour of one of them.

In any case, the Certificate Subject/Signatory is responsible for using the certificate in accordance with its authority and the Relying Party is responsible for verifying its content and scope.

Camerfirma issues these qualified certificates on QSCD devices (card, cryptographic token or cloud) under OID 0.4.0.194112.1.2 according to ETSI EN 319 411-2 - QCP-n-qscd, and on Non-QSCD devices) under OID 0.4.0.194112.1.0 according to ETSI EN 319 411-2 - QCP-n.

- **Certificates For a Public Employee with/without a Pseudonym**

These certificates identify a natural person (Subject/Signatory) as a public employee.

The qualified certificates issued under this CP can be used by the electronic signature systems of the personnel at the service of the Public Administrations, in accordance with the provisions of Article 43 of Law 40/2015, of October 1, on the Legal Regime of the Public Sector.

The certificates issued under these CPs are in accordance with the national regulations of the certificate profiles for public employee and public employee with pseudonym established in sections 10 and 11 of the document "Electronic Certificate Profiles" of the Sub-directorate General for Information, Documentation and Publications of the Ministry of Finance and Public Administrations with the following Policy OIDs according to national regulations:

- in its high levels:
  - employee certificate: OID 2.16.724.1.3.5.7.1
  - employee certificate with pseudonym: OID 2.16.724.1.1.3.5.4.1
- at its medium/substantial level:
  - employee certificate: OID 2.16.724.1.3.5.7.2
  - employee certificate with pseudonym: OID 2.16.724.1.1.3.5.4.2

Camerfirma issues these qualified signature certificates on QSCD devices (card, cryptographic token or cloud) under OID 0.4.0.194112.1.2 according to ETSI EN 319 411-2 -QCP-n-qscd, and on non-QSCD devices under OID 0.4.0.194112.1.0 according to ETSI EN 319 411-2-QCP-n.

Camerfirma issues non-qualified public employee certificates with and without authentication and encryption pseudonym, always in the cloud. These certificates are non-qualified because they cannot be qualified. The Policy OIDs according to national regulations for these certificates are the same as those listed in the previous paragraph. The OID of the non-qualified authentication certificate is 0.4.0.2042.1.2 according to ETSI EN 319 411-1 - NCP+.

This Certification Policy sets out the specific conditions relating to the types of certificates that make up this CP.

1.2 IDENTIFICATION AND NAME OF THE DOCUMENT

Name:	CAMERFIRMA's Certification Policy for Personal Certificates

Description:	Certification policies for personal certificates that generate advanced or qualified electronic signatures.
Version:	See home page
OID:	• **Qualified Citizen Certificate** CHAMBERS OF COMMERCE ROOT Hierarchy - 2016 ○ 1.3.6.1.4.1.1.17326.10.16.1.1.1: QSCD SmartCard/Token ○ 1.3.6.1.1.4.1.1.17326.10.16.1.1.1, 1.3.6.1.4.1.1.17326.99.18.1: QSCD Cloud ○ 1.3.6.1.4.1.1.17326.10.16.1.1.2: No QSCD CAMERFIRMA ROOT 2021 Hierarchy ○ 1.3.6.1.4.1.1.17326.10.21.1.1.1: QSCD SmartCard/Token ○ 1.3.6.1.4.1.1.17326.10.21.1.1.3: QSCD Cloud INFOCERT-CAMERFIRMA ROOT 2024 Hierarchy ○ 1.3.6.1.4.1.1.17326.10.21.1.1.2: No QSCD • **Qualified Corporate / Self-employed / Chartered Self-employed Certificate** CHAMBERS OF COMMERCE ROOT Hierarchy - 2016 ○ 1.3.6.1.4.1.1.17326.10.16.1.2.1: QSCD SmartCard/Token ○ 1.3.6.1.1.4.1.17326.10.16.1.2.1, 1.3.6.1.4.1.1.17326.99.18.1: QSCD Cloud ○ 1.3.6.1.4.1.1.17326.10.16.1.1.2.2 - No QSCD CAMERFIRMA ROOT 2021 Hierarchy ○ 1.3.6.1.4.1.1.17326.10.21.1.2.1: QSCD SmartCard/Token ○ 1.3.6.1.4.1.1.17326.10.21.1.2.3: QSCD Cloud • **Qualified Certificates for a Representative** CHAMBERS OF COMMERCE ROOT Hierarchy - 2016 ○ Legal Representative of a Legal/Non-Legal Entity ▪ 1.3.6.1.4.1.17326.10.16.1.3.1.1: QSCD SmartCard/Token ▪ 1.3.6.1.1.4.1.17326.10.16.1.3.1.1, 1.3.6.1.4.1.1.17326.99.18.1: QSCD Cloud ▪ 1.3.6.1.4.1.1.17326.10.16.1.3.1.2: No QSCD ○ Voluntary Representative of a Legal/Non-Legal Entity before the Public Administrations ▪ 1.3.6.1.4.1.17326.10.16.1.3.2.1: QSCD SmartCard/Token ▪ 1.3.6.1.1.4.1.17326.10.16.1.3.2.1, 1.3.6.1.4.1.1.17326.99.18.1: Cloud QSCD ▪ 1.3.6.1.4.1.17326.10.16.1.3.3.2.2: No QSCD ○ Special Representative of a Legal/Non-Legal Entity ▪ 1.3.6.1.4.1.17326.10.16.1.3.3.1: QSCD SmartCard/Token ▪ 1.3.6.1.1.4.1.17326.10.16.1.3.3.1, 1.3.6.1.4.1.1.17326.99.18.1: QSCD Cloud ▪ 1.3.6.1.4.1.17326.10.16.1.3.3.2: No QSCD CAMERFIRMA ROOT 2021 Hierarchy ○ Legal Representative of a Legal Entity ▪ 1.3.6.1.4.1.1.17326.10.21.1.3.1: QSCD SmartCard/Token ▪ 1.3.6.1.4.1.1.17326.10.21.1.3.3: QSCD Cloud ○ Legal Representative of a Non-Legal Entity ▪ 1.3.6.1.4.1.17326.10.21.1.4.1: QSCD SmartCard/Token ▪ 1.3.6.1.4.1.17326.10.21.1.4.3: QSCD Cloud

- Voluntary Representative of a Legal Entity before the Public Administrations
  - 1.3.6.1.4.1.17326.10.21.1.5.1: QSCD SmartCard/Token
  - 1.3.6.1.4.1.1.17326.10.21.1.5.3: QSCD Cloud
- Voluntary Representative of a Non-Legal Entity before the Public Administrations
  - 1.3.6.1.4.1.1.17326.10.21.1.6.1: QSCD SmartCard/Token
  - 1.3.6.1.4.1.1.17326.10.21.1.6.3: QSCD Cloud
- Special Representative of a Legal Entity
  - 1.3.6.1.4.1.1.17326.10.21.1.7.1: QSCD SmartCard/Token
  - 1.3.6.1.4.1.1.17326.10.21.1.7.3: QSCD Cloud
- Special Representative of a Non-Legal Entity
  - 1.3.6.1.4.1.1.17326.10.21.1.8.1: QSCD SmartCard/Token
  - 1.3.6.1.4.1.1.17326.10.21.1.8.3: QSCD Cloud

- **s Certificates for a Public Employee With/Without a Pseudonym**
  CHAMBERS OF COMMERCE ROOT Hierarchy - 2016
  - Qualified Certificate for Signature - High Level
    - 1.3.6.1.4.1.17326.10.16.1.5.1.3.4.1: QSCD SmartCard/Token
    - 1.3.6.1.1.4.1.17326.10.16.1.5.1.1.3.4.1, 1.3.6.1.4.1.17326.99.18.1: QSCD Cloud
  - Non-Qualified Certificate for Authentication - High Level
    - 1.3.6.1.4.1.17326.10.16.1.5.1.3.4.2: SmartCard/Token
    - 1.3.6.1.4.1.17326.10.16.1.5.1.3.4.2, 1.3.6.1.4.1.17326.99.18.1: Cloud
  - Non-Qualified Certificate for Encipherment - High Level
    - 1.3.6.1.4.1.17326.10.16.1.5.1.3.4.3: SmartCard/Token
    - 1.3.6.1.4.1.17326.10.16.1.5.1.3.4.3, 1.3.6.1.4.1.17326.99.18.1: Cloud
  - Qualified Certificate - Intermediate Level
    - 1.3.6.1.4.1.17326.10.16.1.5.1.1.3.4.4: QSCD SmartCard/Token / No QSCD
    - 1.3.6.1.1.4.1.17326.10.16.1.5.1.3.4.4, 1.3.6.1.4.1.17326.99.18.1: QSCD Cloud
  -

Location: https://www.camerfirma.com/practicas-de-certificacion-ac-camerfirma-cps-dpc/

Previously, this Policy was contained in the general CPD. For a better understanding and management of the documents, this Certification Policy for Personal Certificates is separated and a new version of the CPD is issued, complementary to this CP.

1.3 PKI PARTICIPANTS

1.3.1 CERTIFICATION AUTHORITIES (CA)

Under this CP, Camerfirma manages the following CA hierarchies:

- CHAMBERS OF COMMERCE ROOT:
  - AC CAMERFIRMA FOR NATURAL PERSONS - 2016
- GLOBAL CHAMBERSIGN ROOT

- CAMERFIRMA ROOT 2021
  - AC CAMERFIRMA QUALIFIED CERTIFICATES - 2021
- INFOCERT-CAMERFIRMA ROOT 2024
  - INFOCERT-CAMERFIRMA QUALIFIED CERTIFICATES - 2024

1.3.1.1 TEST CERTIFICATES

As provided in the CPS.

1.3.1.2 INTERNAL MANAGEMENT CA

Camerfirma has developed an internal management CA, called CAMERFIRMA INTERNAL MANAGEMENT, for the issuance of RA operator certificates. With these certificates, operators can perform the actions inherent to their role in the certificate management platform.

The CA CAMERFIRMA INTERNAL MANAGEMENT is outside the scope of this PC.

1.3.2 REGISTRATION AUTHORITIES (RA)

The following types of RA are recognized under this CP:

- AR Cameral: managed directly or under the control of a Spanish Chamber of Commerce, Industry and Navigation.
- Corporate RA: managed by a public organization or a private entity.
- Remote AR: Enterprise AR using third-party applications located in a remote location that communicate, through integration with a web services layer, with the certificate management platform.

Under this CP, they can act as RAs of the Subordinate CAs:

- The CA (Camerfirma).
- The Spanish Chambers of Commerce, Industry and Navigation or the entities designated by them.

  They are obliged to pass the audits required in the contract with the CA.
- Spanish companies, as entities delegated by the CA or by another RA, to which they are contractually bound, to carry out the complete identification and registration of the Applicant and, if applicable, the processing of revocation requests and notifications of revocation-related events, within a given organization or demarcation.

  The operators of these RAs only manage applications and certificates within the scope of their organization or district, unless otherwise determined by the CA or RA to which they report, for example, employees of a corporation, members of a business group or members of a professional association.

  They are obliged to pass the audits required in the contract with the CA.
- Entities belonging to the Spanish Public Administrations.

They are obliged to pass the audits required in the contract with the CA.

- Other legal entities or agents, Spanish or international, that have a contractual relationship with the CA.

  For the issuance of certificates to individuals or legal entities that do not reside in Spanish territory, a legal report may be required to justify the correct fulfillment of the identification and registration requirements.

  They are obliged to pass the audits required in the contract with the CA.

- PVP. On-Site Verification Point that always depends on a RA. It may be a legal entity or a natural person to whom the RA partially delegates the identification tasks.

  Their main mission is to identify the Applicant by personal appearance and to deliver the identification documentation to the RA. For these functions the PVPs are not subject to training or controls.

  Occasionally, the PVP's functions may be extended to the collection and collation of the documentation submitted by the Applicant, verification of its suitability for the type of certificate requested and delivery of this documentation to the RA on which it depends, but a PVP can never validate the registration process and decide on the issuance of the certificate.

  A RA operator checks, according to the applicable CP, the documentation provided by the PVP and, if applicable, the documentation submitted directly to the RA, and, if correct, proceeds with the issuance of the certificate by the CA, without the need to perform a new identification of the Applicant.

  Since a PVP has no registration capacity, it is contractually bound to a RA through a contract. Camerfirma has drawn up a standard relationship document between the RA and the PVP, which defines the functions that the RA delegates to the PVP.

- PVR. Remote Verification Point that always depends on a RA. It can be a legal entity or a natural person to whom the RA partially delegates the identification tasks.

  Their main mission is to identify the Applicant by means of remote video identification processes, which may be used to issue qualified certificates, provided they comply with the conditions and technical requirements required by the applicable standard. For these functions, the PVRs are subject to specific training and controls.

  Occasionally, the PVR may see its functions extended to the reception and collation of the documentation submitted by the Applicant, verification of its suitability for the type of certificate requested and delivery of this documentation to the RA on which it depends, but a PVR can never validate the registration process and decide on the issuance of the certificate.

  Upon receipt of the evidence of identification provided by the PVR, a RA operator checks, according to the applicable CP, the documentation provided by the PVR and/or, if applicable, the documentation submitted directly to the RA, and, if correct, proceeds with the issuance of the certificate by the CA, without the need to perform a new identification

of the Applicant.

Since a PVR has no registration capacity, it is contractually bound to a RA through a contract. Camerfirma has drawn up a standard relationship document between the RA and the PVR defining the functions that the RA delegates to the PVR.

1.3.3 SUBSCRIBERS

1.3.3.1 SUBSCRIBER

Under this CP, the Subscriber of a certificate may be:

- For certificates issued to natural persons without linkage attributes to an Entity:
  - The natural person Subject.
  - A legal entity or an entity without legal personality to which the natural person Subject is linked.
- For certificates issued to natural persons with binding attributes to an Entity (legal person or entity without legal personality):
  - The natural person Subject.
  - The Entity (legal person or unincorporated entity) identified in the certificate to which the natural person Subject is linked.
  - A legal entity or an entity without legal personality to which the natural person Subject is linked (other than the Entity identified in the certificate).

To avoid a conflict of interest, the Subscriber of a certificate and Camerfirma, as the certificate issuing CSP (CA under this CP), or the RAs under this CP must be independent entities. The only exceptions are:

- A third organization acting as RA under this CP and as Subscriber of the certificates issued to the Subjects bound to it.
- Certificates that Camerfirma issues for itself (as a legal entity) or for individuals that are part of it (as a Subject).

For both exceptions, the application, validation and processing of certificates must be carried out according to the processes defined by Camerfirma for the respective types of certificates.

1.3.3.2 SUBJECT AND SIGNATORY

Under this CP, a Certificate Subject may be:

- For certificates issued to natural persons without linkage attributes to an Entity:
  - The natural person to whom the certificate is issued. The Subscriber can be:

        - The Subject (the natural person identified in the certificate).
        - A legal person or an entity without legal personality to which the Subject is linked.
- For certificates issued to natural persons with binding attributes to an Entity (legal person or entity without legal personality):
    - The natural person to whom the certificate is issued. The Subscriber can be:
        - The Subject (the natural person identified in the certificate).
        - The Entity identified in the certificate to which the Registrant is bound (the legal person or unincorporated entity identified in the certificate).
        - A legal entity or an entity without legal personality to which the Subject is linked (other than the Entity identified in the certificate).

Under this CP, and in accordance with the eIDAS Regulation, the Signatory is the natural person identified in an electronic signature certificate.

Under these CPs, the Signatory of a certificate can be:

- For certificates issued to natural persons, with or without binding attributes to an Entity, qualified or non-qualified with permitted use of signature:
    - The Signatory is the natural person Subject (the natural person identified in the certificate).
- For other certificates issued to natural persons (non-qualified authentication or encryption certificates, with binding attributes to an Entity, without permitted signature use).
    - No Signatory.

The Signatory, as the natural person holding the electronic signature certificate, shall be directly responsible for the obligations associated with the use and management of the certificate and its associated private key.

In this CP, the term "Subject/Signatory" refers, generically, to the Subject and/or Signatory of certificates issued to natural persons.

1.3.3.3 APPLICANT

Under these CPs, the Applicant for a certificate shall be the natural person who is the certificate Subject.

1.3.4 RESPONSIBLE

Under this CP, the Responsible Party is the natural person responsible for the use of the private key associated with the public key contained in a certificate.

During the certificate issuance process, the Responsible person performs, among the following

functions, those applicable to the type of device where the certificate keys are generated: deliver the public key, receive the private key, define and/or receive the private key activation data, receive the certificate.

Under these CPs, the Person Responsible for a certificate may be the Applicant, or a natural person authorized by the Applicant, without prejudice to the obligations of the Signatory and, if applicable, the Registrant.

1.3.5 RELYING PARTIES

In this CP, the Relying Party is the person or organization that voluntarily relies on a certificate issued by any of the CAs under this CP.

1.3.6 OTHER PARTICIPANTS

1.3.6.1 *SUPERVISORY BODY*

As provided in the CPS.

1.4 CERTIFICATE USAGEE

1.4.1 APPROPRIATE USES OF CERTIFICATES

Certificates issued under these CPs are used for the following purposes:

- Authentication of the Subject.
- Qualified electronic signature or advanced electronic signature, depending on whether the certificate is issued on qualified electronic signature creation devices or not.
- Asymmetric or mixed encryption without key recovery.

1.4.2 PROHIBITED USES OF CERTIFICATES

Camerfirma incorporates information on the limitation of use in the certificates, either in the standard extensions "*Key Usage*" and "*Basic Constraints*", marked as "critical" in the certificate and, therefore, of mandatory compliance by the applications that use the certificate, or limitations in standard extensions such as "*Extended Key Usage*" and "*Name Constraints*" and/or by means of texts incorporated in the "*User Notice*" field in the standard extension "*Certificate Policies*", marked as "non-critical" in the certificate, but of mandatory compliance by the Certificate Subject and the Relying Parties.

The certificates may only be used within the limits and for the purposes for which they have been issued and which are described in this document.

The certificates are not designed (they are not intended and are not authorized for use or resale) as hazardous situation monitoring equipment or for uses requiring fail-safe performance, such as the operation of nuclear facilities, airborne navigation or communications systems, or weapons control systems, where failure could directly result in death, personal injury or severe

environmental damage.

The use of the certificates in operations that contravene the CP applicable to each one of the certificates, the CPD, the Terms and Conditions or the CA's contracts with the RAs or with the Subscribers shall be considered as improper use, for the appropriate legal purposes, therefore exempting the CA, according to the legislation in force, from any liability for this improper use of the certificates made by the Subjects or any third party.

Camerfirma does not have access to the data on which the use of a certificate can be applied. Therefore, and as a consequence of this technical impossibility to access the message content, Camerfirma cannot issue any assessment of said content, and therefore the Data Controller assumes any liability arising from the content associated with the use of a certificate. Likewise, any liability that may arise from the use of the same outside the limits and conditions of use contained in this document and in the Terms and Conditions, as well as any other improper use of the same derived from this section or that may be interpreted as such according to the legislation in force, shall be attributable to the Subject.

The private key of the certificates is stored by Camerfirma only for Cloud certificates, so in other cases, it is not possible to recover the encrypted data with the corresponding public key in the event of loss of the certificate's private key by the certificate Subject. If the Subject encrypts the data with the public key, he/she does so under his/her sole and exclusive responsibility.

1.5 POLICY ADMINISTRATION

As provided in the CPS.

1.5.1 ORGANIZATION MANAGING THE DOCUMENT

As provided in the CPS.

1.5.2 CONTACT INFORMATION

As provided in the CPS.

1.5.3 PERSON WHO DETERMINES CPS SUITABILITY FOR THE POLICY

As provided in the CPS.

1.5.4 DOCUMENT MANAGEMENT PROCEDURES

As provided in the CPS.

1.6 DEFINITIONS AND ACRONYMS

As provided in the CPS

2 PUBLICATION AND RESPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

Camerfirma's repositories for the publication of certification information are available 24 hours a day, 7 days a week.

In the event of system failure, or any other factor beyond Camerfirma's control, Camerfirma will make every effort to ensure that these repositories are not inaccessible for more than 24 hours.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

2.2.1 CERTIFICATION POLICIES AND PRACTICES

Camerfirma makes the current version of this CP available to the public on the following website:

- https://www.camerfirma.com/practicas-de-certificacion-ac-camerfirma-cps-dpc/
- https://policy.camerfirma.com
- https://policy2021.camerfirma.com

Once a new version of this CP is published, Camerfirma will keep the previous version available to the public on the same website, at least until the completion of all the CAs included in that version.

2.2.2 TERMS AND CONDITIONS

As provided in the CPS

2.2.3 DISSEMINATION OF CERTIFICATES

As provided in the CPS.

2.2.4 CRL AND OCSP

As provided in the CPS.

2.3 FREQUENCY OF PUBLICATION

As provided in the CPS.

2.4 REPOSITORY ACCESS CONTROLS

As provided in the CPS.

3 IDENTIFICATION AND AUTHENTICATION

3.1 DESIGNATION

3.1.1 TYPES OF NAMES

The Registrant data (names) are included in the *Subject* field of the certificate, by means of a *Distinguished Name* (DN) according to the X.500 reference standard in ISO/IEC 9594 and, if applicable, in the fields of the *Subject Alternative Name* extension of the certificate.

The structure and content of the DN in the *Subject* field and, if applicable, of the fields in the *Subject Alternative Name* extension are described in the certificate profile sheets, including as a minimum:

- For end-entity certificates issued to individuals without Entity binding attributes:
  - Name and surname and tax identification number of the natural person.
- For end entity certificates issued to natural persons with attributes of linkage to an Entity (legal person or entity without legal personality):
  - Name and surname and tax identification number of the natural person.
  - Company name and fiscal identifier of the Entity.

  This rule does not apply to certificates with a pseudonym, which must identify this condition.

The certificate profile files under this CP can be requested through Camerfirma's customer support service at https://www.camerfirma.com/contacto-soporte or by calling +34 91 136 91 05.

3.1.2 MEANING OF NAMES

All DNs are meaningful, and the identification of the attributes associated with the Subject is in a human readable form. The fields of the DN referring to the "name and surname" of the Subject must be the same as the data presented by means of the reliable identity document, and with the same format.

3.1.3 ANONYMITY OR PSEUDONYMITY OF SUBSCRIBERS

Camerfirma will use the pseudonym in those certificates where it is allowed in the *CN* and *pseudonym* attributes of the DN, confidentially keeping the real identity of the Subject/Signatory.

The pseudonym is calculated in such a way as to uniquely identify the authentic Subject/Signatory.

3.1.4 RULES USED TO INTERPRET VARIOUS NAME FORMATS

As provided in the CPS.

3.1.5 UNIQUENESS OF NAMES

As provided in the CPS.

3.1.6 NAME CONFLICT RESOLUTION PROCEDURE

As provided in the CPS.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 METHODS OF PROOF OF POSSESSION OF THE PRIVATE KEY

Before issuing a certificate, it is mandatory to verify the identity of the applicant by presenting a valid identity document. The documents accepted vary according to the nationality and status of the applicant:

- Spanish Nationality: National Identity Card or Passport.
- EU or EEA foreigners with NIE: Passport or national identity card issued by an EU or EEA country and Certificate of Foreigner Identity Number (NIE).
- EU or EEA foreigners without NIE but with NIF: Passport or national identity card issued by an EU or EEA country and Tax Identification Number Certificate (NIF).
- EU or EEA foreigners without NIE or NIF: Passport or national identity card issued by an EU or EEA country.
- Foreigners from other countries residing in Spain (with NIE): Residence Card or Foreigner's Identity Card with photograph.
- Foreigners from other countries not residing in Spain (without NIE) but with NIF: Passport and Tax Identification Number Certificate (NIF).

Certificates cannot be issued to minors who are not emancipated, or who are judicially incapacitated in whole or in part, or when there are well-founded suspicions that the Applicant is not in possession of his or her full mental capacity.

Authentication can be performed using different methods in accordance with the eIDAS Regulation and national regulations:

- Physical appearance before the Certification Authority (CA), Registration Authority (RA) or in a Presential Verification Point (PVP). Appearance before a notary with a notarized signature is also accepted.
- Remote electronic identification, by means of identification systems notified by the Member States under Article 9.1 of the eIDAS Regulation, provided that they meet a "high" security level. In Spain, the electronic ID has been notified.
- Use of qualified electronic signature with a certificate issued by a Camerfirma CA or another PCSC, provided that they contain the applicant's identity data.
- Remote video identification methods, in accordance with Order ETD/465/2021, including assisted (operator-assisted) and unassisted (later revision) processes.

  In these remote video identification processes, Camerfirma will be able to verify the applicant's data with official sources, store audio/video records and apply restrictions on the acceptance of identity documents.

The provisions of this section on the obligation to verify the identity of the Applicant of a qualified certificate may not be required when the identity or other permanent circumstances of the Applicant were already known to Camerfirma or the RA by virtue of a pre-existing relationship, in which, for the identification of the Applicant, face-to-face identification was used and the period of time elapsed since the identification was less than five years.

For non-qualified certificates, in addition to the above methods, identification by means of advanced electronic signatures or video identification methods not recognized at national level may be accepted.

3.2.2 AUTHENTICATION OF THE ORGANIZATION'S IDENTITY

As provided in the CPS

3.2.3 AUTHENTICATION OF THE IDENTITY OF THE NATURAL PERSON APPLICANT

As provided in the CPS

3.2.4 UNVERIFIED SUBSCRIBER INFORMATION

It is not allowed to include unverified information in the *Subject* field of a certificate.

3.2.5 AUTHORITY VALIDATION

3.2.5.1 VERIFICATION OF THE LINK OF THE APPLICANT AND THE PERSON RESPONSIBLE TO THE ENTITY.

Camerfirma must verify the link between the applicant of a natural person certificate and the company and organization he/she represents or to which he/she is adhered or registered, through the following documentation:

Type of certificate	Documentation
Qualified Corporate Certificate	Usually, authorization signed by anEntity's legal representative.
Qualified Corporate Certificate for a Self-employed Qualified Corporate Certificate for a Chartered Self-employed	Documentation accrediting the status of self-employed in economic activity regime, and if you are a professional member of a professional association (subscription in force). Optionally, documentation accrediting the registered trade name under which the activity is carried out.
Qualified Certificate for a Representative of a Legal/Non-Legal Entity with general powers of representation	Documentation accrediting the powers of representation of the Entity, depending on the type of representative and the type of Entity.

Qualified Certificate for a Voluntary Representative of a Legal/Non-Legal Entity before the Public Administrations Qualified Certificate for a Special Representative of a Legal/Non-Legal Entity	
Certificates for a Public Employee With/Without a Pseudonym	Authorization signed by a person with powers of representation of the Entity indicating tha the/she is a public employee, or appointment in the Official State Gazette where this person's DNI/NIE No. appears.
Non Qualified Certificate for Personnel for Public Administrations	Authorization signed by a person with powers of representation of the Entity indicating that he/she is a public employee, or appointment in the Official Gazette where the DNI/NIE of this person is stated.

3.2.5.2 *SPECIAL CONSIDERATIONS FOR THE ISSUANCE OF CERTIFICATES OUTSIDE SPANISH TERRITORY*

The documentation required for this purpose is that which is legally applicable in each country as long as it allows compliance with the corresponding identification obligation in accordance with Spanish legislation.

3.2.6 CRITERIA FOR INTEROPERATION

As provided in the CPS.

3.3 IDENTIFICATION AND AUTHENTICATION OF RENEWAL REQUESTS WITH CHANGE OF PASSWORDS

As provided in the CPS

3.3.1 IDENTIFICATION AND AUTHENTICATION OF A RENEWAL REQUEST WITH ROUTINE KEY CHANGE

As provided in the CPS

3.3.2 IDENTIFICATION AND AUTHENTICATION OF A RENEWAL APPLICATION WITH CHANGE OF KEYS AFTER REVOCATION

As provided in the CPS

3.4 IDENTIFICATION AND AUTHENTICATION OF A REVOCATION REQUEST

As provided in the CPS

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

Request for certificates

4.1.1 WHO CAN APPLY FOR A CERTIFICATE

A certificate request may be submitted by the Applicant, with the participation, if any, of the Controller, and/or the Registrant, and/or the Subscriber or the Entity.

4.1.2 CERTIFICATE APPLICATION PROCESS AND RESPONSIBILITIES

Certificate applications are generally made by accessing the application forms on Camerfirma's website, or by sending the Applicant or the Controller a link to a specific form.

The web page contains the necessary forms to request each type of certificate distributed by Camerfirma in different formats and the signature generation devices, if necessary.

The form will allow the incorporation of a CSR (PKCS #10) in case the Subject has created the keys in an external device not managed by Camerfirma.

The Responsible, and the Subject if different, receive, after the confirmation of the request data, an email in the account associated to the certificate request a link to confirm the request and accept the Terms and Conditions.

Once the application has been confirmed, the Applicant is informed of the documentation to be presented at an authorized registration office and to comply with the requirement of face-to-face identification if applicable.

4.2 PROCESSING OF CERTIFICATE APPLICATIONS

4.2.1 EXECUTION OF IDENTIFICATION AND AUTHENTICATION FUNCTIONS

As provided in the CPS

4.2.2 APPROVAL OR REJECTION OF THE APPLICATION

As provided in the CPS

4.2.3 DEADLINE TO RESOLVE THE REQUEST

As provided in the CPS

4.3 ISSUANCE OF CERTIFICATES

4.3.1 CA ACTIONS DURING THE ISSUANCE PROCESS

As provided in the CPS.

4.3.2 NOTIFICATION OF CERTIFICATE ISSUANCE TO THE SUBSCRIBER

For certificates issued under this COP, the Responsible is notified by e-mail indicating the approval or denial of the request.

4.4 ACCEPTANCE OF CERTIFICATES

4.4.1 CONDUCT THAT CONSTITUTES ACCEPTANCE OF THE CERTIFICATE

As provided in the CPS

4.4.2 PUBLICATION OF THE CERTIFICATE BY THE CA

As provided in the CPS

4.4.3 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

According to the provisions of the CPS

4.5 USE OF KEY PAIR AND CERTIFICATES

4.5.1 SUBSCRIBER PRIVATE KEY AND CERTIFICATE USAGE

The key usage limitation is defined in the certificate content in the extensions: *Key Usage*, *Extended Key Usage* and *Basic Constraints*.

AC/PC	Key Usage	Extended Key Usage	Basic Constraints
CHAMBERS OF COMMERCE ROOT - 2016	critical, cRLSign, keyCertSign	-	critical, CA:true
AC CAMERFIRMA FOR NATURAL PERSONS - 2016	critical, cRLSign, keyCertSign	emailProtection clientAuth	critical, CA:true, pathLen:2
Qualified Citizen Certificate - QSCD SmartCard/Token, QSCD Cloud, Non-QSCD	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical, CA:false
Qualified Corporate Certificate / Qualified Certificate for a Self-employed / Qualified Certificate for a Chartered Self-employed - QSCD SmartCard/Token, QSCD Cloud, Non-QSCD	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical, CA:false
Qualified Certificate for a Legal Representative of a Legal/Non-Legal Entity – QSCD SmartCard/Token, QSCD Cloud, Non-QSCD	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical, CA:false
Qualified Certificate for a Voluntary Representative of a	critical, digitalSignature,	emailProtection clientAuth	critical, CA:false

Legal/Non-Legal Entity before the Public Administrations - QSCD SmartCard/Token, QSCD Cloud, Non-QSCD	contentCommitment, keyEncipherment		
Qualified Certificate for a Special Representative of a Legal/Non-Legal Entity - QSCD SmartCard/Token, QSCD Cloud, Non-QSCD	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical, CA:false
Qualified Certificate for Signature for a Public Employee With/Without a Pseudonym - High Level - QSCD SmartCard/Token, QSCD Cloud	critical, contentCommitment	-	critical, CA:false
Non-Qualified Certificate for Authentication for a Public Employee With/Without a Pseudonym - High Level - SmartCard/Token, Cloud	critical, digitalSignature	emailProtection clientAuth	critical, CA:false
Non-Qualified Certificate for Encipherment for a Public Employee With/Without a Pseudonym - High Level - SmartCard/Token, Cloud	critical, keyEncipherment, dataEncipherment	emailProtection clientAuth	critical, CA:false
Qualified Certificate for a Public Employee With/Without a Pseudonym - Medium Level - QSCD SmartCard/Token / Non-QSCD, QSCD Cloud	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical, CA:false
CAMERFIRMA ROOT 2021	critical, cRLSign, keyCertSign	-	critical, CA:true
AC CAMERFIRMA QUALIFIED CERTIFICATES - 2021	critical, cRLSign, keyCertSign	emailProtection, clientAuth	critical, CA:true, pathLen:0
Qualified Citizen Certificate - QSCD SmartCard/Token, QSCD Cloud	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection, clientAuth	critical, CA:false
Qualified Corporate Certificate - QSCD SmartCard/Token, QSCD	critical, digitalSignature, contentCommitment,	emailProtection, clientAuth	critical, CA:false

Cloud	keyEncipherment		
Qualified Certificate for a Legal Representative of a Legal Entity - QSCD SmartCard/Token, QSCD Cloud	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection, clientAuth	critical, CA:false
Qualified Certificate for a Legal Representative of a Non-Legal Entity - QSCD SmartCard/Token, QSCD Cloud	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection, clientAuth	critical, CA:false
Qualified Certificate for a Voluntary Representative of a Legal Entity before the Public Administrations - QSCD SmartCard/Token, QSCD Cloud	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection, clientAuth	critical, CA:false
Qualified Certificate for a Voluntary Representative of a Non-Legal Entity before the Public Administrations - QSCD SmartCard/Token, QSCD Cloud	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection, clientAuth	critical, CA:false
Qualified Certificate for a Special Representative of a Legal Entity - QSCD SmartCard/Token, QSCD Cloud	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection, clientAuth	critical, CA:false
Qualified Certificate for a Special Representative of a Non-Legal Entity - QSCD SmartCard/Token, QSCD Cloud	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection, clientAuth	critical, CA:false
INFOCERT-CAMERFIRMA CERTIFICATES 2024	critical, cRLSign, keyCertSign	-	critical, CA:true
INFOCERT-CAMERFIRMA QUALIFIED CERTIFICATES - 2024	critical, cRLSign, keyCertSign	Adobe Trust, clientAuth	critical, CA:true, pathLen:0
Qualified Citizen Certificate - No QSCD	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical, CA:false

Although it is technically possible to encrypt data with the certificates, Camerfirma is not liable for damages caused by the loss of control of the Subject of the private key required to decrypt the information, except in the certificate issued exclusively for this use.

For remote signature certificates, the Registrant/Signatory must keep the remote signature authentication tools and/or devices secure. Likewise, he/she must keep the remote signature certificate's private key activation PIN under his/her exclusive control and separate from the authentication passwords or authentication devices. Finally, the privacy and preservation of the certificate revocation PIN must be ensured. The Registrant/Signatory must not create digital signatures with private keys of suspended or revoked certificates or use revoked CA certificates.

4.5.2 RELYING PARTY PUBLIC KEY AND CERTIFICATE USAGE

As provided in the CPS

4.6 CERTIFICATE RENEWAL

4.6.1 CIRCUMSTANCES FOR CERTIFICATE RENEWAL

Not stipulated.

4.6.2 WHO MAY REQUEST RENEWAL

Not stipulated.

4.6.3 PROCESSING OF CERTIFICATE RENEWAL REQUESTS

Not stipulated.

4.6.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

Not stipulated.

4.6.5 CONDUCT CONSTITUTING ACCEPTANCE OF THE RENEWAL CERTIFICATE

Not stipulated.

4.6.6 PUBLICATION OF THE RENEWAL CERTIFICATE BY THE CA

Not stipulated.

4.6.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

Not stipulated.

4.7 CERTIFICATE RE-KEY

As provided in the CPS.

4.7.1 CIRCUMSTANCES FOR CERTIFICATE RE-KEY

For certificates issued under this CP, a certificate may be renewed with a key change prior to its expiration date.

Renewal of a certificate is not allowed, and instead a new issuance of the certificate must be made in the following cases:

- The certificate has expired.
- The certificate has been revoked.
- The data of the Subject/Signatory in the certificate has changed. EXCEPTION: in cases of renewal of a certificate when its expiration date is near and in some cases of replacement of a certificate, it is allowed to change the email address contained in the certificate.
- In the case of a qualified certificate, more than 4 years have elapsed since the last face-to-face identification of the Applicant.

4.7.2 WHO MAY REQUEST FOR CERTIFICATE RE-KEY

As provided in the CPS.

4.7.3 PROCESSING CERTIFICATE RE-KEYING REQUEST

As provided in the CPS

4.7.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

As provided in the CPS

4.7.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RE-KEY CERTIFICATE

According to the provisions of the CPS

4.7.6 PUBLICATION OF THE RE-KEYED CERTIFICATE BY THE CA

As provided in the CPS

4.7.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

As provided in the CPS

4.8 CERTIFICATE MODIFICATION

Any need to modify data of the Subject in a certificate requires a new certificate request. A new certificate will be issued with new keys and corrected data and, if necessary, the old certificate will be revoked.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

As provided in the CPS

4.9.1 CIRCUMSTANCES FOR REVOCATION

As provided in the CPS

4.9.2 WHO CAN REQUEST REVOCATION

As provided in the CPS

4.9.3 PROCEDURE FOR REVOCATION REQUEST

As provided in the CPS.

4.9.4 REVOCATION REQUEST GRACE PERIOD

As provided in the CPS

4.9.5 TIME WITHIN WHICH THE CA MUST PROCESS THE REVOCATION REQUEST

As provided in the CPS

4.9.6 REVOCATION CHECKING REQUIREMENT FOR RELYING PARTIES

As provided in the CPS

4.9.7 CRL ISSUANCE FREQUENCY

As provided in the CPS

4.9.8 MAXIMUM LATENCY FOR CRL

As provided in the CPS.

4.9.9 ON-LINE REVOCATION/STATUS CHECKING AVAILABILITY

As provided in the CPS

4.9.10 ON-LINE REVOCATION CHECKING REQUIREMENTS

As provided in the CPS

4.9.11 OTHER FORMS OF REVOCATION ADVERTISEMENTS AVAILABLE

As provided in the CPS

4.9.12 SPECIAL REQUIREMENTS REGARDING KEY COMPROMISE

As provided in the CPS

4.9.13 CIRCUMSTANCES FOR SUSPENSION

As provided in the CPS

4.9.14 WHO CAN REQUEST THE SUSPENSION

As provided in the CPS

4.9.15 PROCEDURE FOR SUSPENSION REQUEST

As provided in the CPS

4.9.16 LIMITS OF THE SUSPENSION PERIOD

As provided in the CPS

4.10 CERTIFICATE STATUS CHECKING SERVICES

4.10.1 OPERATIONAL CHARACTERISTICS

As provided in the CPS.

4.10.2 SERVICE AVAILABILITY

As provided in the CPS.

4.11 END OF SUBSCRIPTION

As provided in the CPS.

4.12 KEY ESCROY AND RECOVERY

4.12.1 KEY ESCROW AND RECOVERY POLICY AND PRACTICES

As provided in the CPS.

4.12.2 SESSION KEY ENCAPSULATION AND RECOVERY POLICY AND PRACTICES

Not stipulated.

5 FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

As provided in the CPS.

5.1.1 LOCATION AND CONSTRUCTION

As provided in the CPS.

5.1.2 PHYSICAL ACCESS

As provided in the CPS.

5.1.3 POWER SUPPLY AND AIR CONDITIONING

As provided in the CPS.

5.1.4 WATER EXPOSURE

As provided in the CPS.

5.1.5 FIRE PROTECTION AND PREVENTION

As provided in the CPS.

5.1.6 STORAGE SYSTEM

As provided in the CPS.

5.1.7 WASTE DISPOSAL

As provided in the CPS.

5.1.8 OFF-SITE BACKUP

As provided in the CPS.

5.2 PROCEDURAL CONTROLS

5.2.1 TRUSTED ROLES

As provided in the CPS.

5.2.2 NUMBER OF PERSONS REQUIRED PER TASK

As provided in the CPS.

5.2.3 IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE

As provided in the CPS.

5.2.4 ROLES REQUIRING SEGREGATION OF DUTIES

As provided in the CPS.

5.3 PERSONNEL CONTROLS

5.3.1 QUALIFICATIONS, EXPERIENCE AND LICENSING REQUIREMENTS

As provided in the CPS.

5.3.2 BACKGROUND CHECK PROCEDURES

As provided in the CPS.

5.3.3 TRAINING REQUIREMENTS

As provided in the CPS.

5.3.4 RETRAINING FREQUENCY AND REQUIREMENTS

As provided in the CPS.

5.3.5 JOB ROTATION FREQUENCY AND SEQUENCE

Not stipulated.

5.3.6 SANCTIONS FOR UNAUTHORIZED ACTIONS

As provided in the CPS.

5.3.7 INDEPENDENT CONTRACTOR REQUIREMENTS

As provided in the CPS.

5.3.8 DOCUMENTATION SUPPLIED TO PERSONNEL

As provided in the CPS.

5.4 AUDIT LOGGING PROCEDURES

As provided in the CPS.

5.4.1 TYPES OF EVENTS RECORDED

As provided in the CPS.

5.4.2 RETENTION PERIODS FOR AUDIT LOGS

As provided in the CPS.

5.4.3 PROTECTION OF AUDIT LOG

As provided in the CPS.

5.4.4 AUDIT LOG BACKUP PROCEDURES

As provided in the CPS.

5.4.5 AUDIT COLLECTION SYSTEM (INTERNAL VS. EXTERNAL)

As provided in the CPS.

5.4.6 NOTIFICATION TO EVENT-CAUSING SUBJECT

As provided in the CPS.

5.4.7 VULNERABILITY ASSESSMENTS

As provided in the CPS.

5.5 RECORDS ARCHIVAL

5.5.1 TYPE OF REGISTERED ARCHIVED

As provided in the CPS.

5.5.2 RETENTION PERIOD FOR ARCHIVE

As provided in the CPS.

5.5.3 PROTECTION OF ARCHIVE

As provided in the CPS.

5.5.4 ARCHIVE BACKUP PROCEDURES

As provided in the CPS.

5.5.5 REQUIREMENTS FOR TIME-STAMPING OF RECORDS

As provided in the CPS.

5.5.6 AUDIT INFORMATION COLLECTION SYSTEM (INTERNAL OR EXTERNAL)

Not stipulated.

5.5.7 PROCEDURES TO OBTAIN AND VERIFY ARCHIVE INFORMATION

As provided in the CPS.

5.6 KEY CHANGEOVER

As provided in the CPS.

5.7 COMPROMISE AND DISASTER RECOVERY

As provided in the CPS.

5.7.1 INCIDENT AND COMPROMISE HANDLING PROCEDURES

As provided in the CPS.

5.7.2 COMPUTING RESOURCES, SOFTWARE, AND/OR DATA ARE CORRUPTED

As provided in the CPS.

5.7.3 COMPROMISE OF THE PRIVATE KEY OF THE CA

As provided in the CPS.

5.7.4 BUSINESS CONTINUITY AFTER A DISASTER

As provided in the CPS.

5.8 CA OR RA

5.8.1 CESSATION OF ACTIVITY

As provided in the CPS.

5.8.2 TERMINATION OF A CA

As provided in the CPS.

5.8.3 TERMINATION OF A RA

As provided in the CPS.

6 TECHNICAL SECRURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 KEY PAIR GENERATION

As provided in the CPS.

6.1.2 PRIVATE KEY DELIVERY TO SUBSCRIBER

As provided in the CPS.

6.1.3 PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER

As provided in the CPS.

6.1.4 CA PUBLIC KEY DELIVERY TO RELYING PARTIES

As provided in the CPS.

6.1.5 KEY SIZES

As provided in the CPS.

6.1.6 PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING

As provided in the CPS.

6.1.7 KEY USAGE PURPOSES

As provided in the CPS.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 CRYPTOGRAPHIC MODULE STANDARDS AND CONTROLS

As provided in the CPS.

6.2.2 PRIVATE KEY (N OUT OF M) MULTI-PERSON CONTROL

As provided in the CPS.

6.2.3 PRIVATE KEY ESCROW

As provided in the CPS.

6.2.4 PRIVATE KEY BACKUP

As provided in the CPS.

6.2.5 PRIVATE KEY ARCHIVAL

As provided in the CPS.

6.2.6 PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE

As provided in the CPS.

6.2.7 PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE

As provided in the CPS.

6.2.8 METHOD OF ACTIVATING PRIVATE KEY

As provided in the CPS.

6.2.9 METHOD OF DEACTIVATING PRIVATE KEY

As provided in the CPS.

6.2.10 METHOD OF DESTROYING PRIVATE KEY

As provided in the CPS.

6.2.11 QUALIFICATION OF THE CRYPTOGRAPHIC MODULE

As provided in the CPS.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 PUBLIC KEY ARCHIVAL

As provided in the CPS.

6.3.2 CERTIFICATE OPERATIONAL PERIODS AND KEY PAIR USAGE PERIODS

As provided in the CPS.

6.4 ACTIVATION DATA

6.4.1 ACTIVATION DATA GENERATION AND INSTALLATION

As provided in the CPS.

6.4.2 ACTIVATION DATA PROTECTION

As provided in the CPS.

6.4.3 OTHER ASPECTS OF ACTIVATION DATA

Not stipulated.

6.5 COMPUTER SECURITY CONTROLS

As provided in the CPS.

6.5.1 SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS

As provided in the CPS.

6.5.2 COMPUTER SECURITY RATING

As provided in the CPS.

6.6 LIFE CYCLE TECHNICAL CONTROLS

As provided in the CPS.

6.6.1 SYSTEM DEVELOPMENT CONTROLS

As provided in the CPS.

6.6.2 SECURITY MANAGEMENT CONTROLS

As provided in the CPS.

6.6.3 CRYPTOGRAPHIC HARDWARE LIFECYCLE MANAGEMENT

As provided in the CPS.

6.6.4 LIFE CYCLE SAFETY ASSESSMENT

Not stipulated.

6.7 NETWORK SECURITY CONTROLS

As provided in the CPS.

6.8 TIME-STAMPING

As provided in the CPS.

7 CERTIFICATE, CRL AND OCSP PROFILES

7.1 CERTIFICATE PROFILES

As provided in the CPS.

7.1.1 VERSION NUMBER

All certificates are X.509 version 3.

7.1.2 CERTIFICATE EXTENSIONS

As provided in the CPS.

7.1.3 ALGORITHM OBJECT IDENTIFIERS

As provided in the CPS.

7.1.4 NAME FORMS

The certificates contain the data of the Subject (names) that are necessary for their use in the *Subject* field and, if applicable, in the *Subject Alternative Name* extension, in accordance with the provisions of this CP.

In general, public employee certificates must include the following data of the Subject in the *Subject* field and, if applicable, in the extension *Subject Alternative Name :*

- If applicable, name and surname of the natural person Subject in separate fields.
- If applicable, corporate name of the Entity (legal entity or entity without legal personality).
- Identity document numbers of the natural person and/or the Entity, in accordance with the applicable legislation.

This rule does not apply to certificates with a pseudonym, which must identify this condition.

The format and semantics of the data included in the *Subject* field and, if applicable, in the *Subject Alternative Name* extension are described in the certificate profile sheets.

7.1.5 NAME CONSTRAINTS

As provided in the CPS.

7.1.6 CERTIFICATION POLICY OBJECT IDENTIFIER (OID)

As provided in the CPS.

7.1.7 USE OF THE POLICY CONSTRAINTS EXTENSION

As provided in the CPS.

7.1.8 POLICY QUALIFIERS SYNTAX AND SEMANTICS

As provided in the CPS.

7.1.9 PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICIES EXTENSION

As provided in the CPS.

7.2 CRL PROFILES

As provided in the CPS.

7.2.1 VERSION NUMBER

As provided in the CPS.

7.2.2 CRL AND CRL ENTRY EXTENSIONS

As provided in the CPS.

7.3 OCSP PROFILES

As provided in the CPS.

7.3.1 VERSION NUMBER

As provided in the CPS.

7.3.2 OCSP EXTENSIONS

As provided in the CPS.

8 COMPLIANCE AUDITS AND OTHER ASSESSMENTS

As provided in the CPS.

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

As provided in the CPS.

8.1.1 EXTERNAL SUBORDINATE CA AUDITS OR CROSS CERTIFICATION.

Not applicable.

8.1.2 AUDITING THE RAS

As provided in the CPS.

8.1.3 INTERNAL AUDITS

As provided in the CPS.

8.2 IDENTITY/QUALIFICATIONS OF AUDITORS

As provided in the CPS.

8.3 RELATIONSHIP BETWEEN THE AUDITOR AND THE AUDITED ENTITY

As provided in the CPS.

8.4 TOPICS COVERED BY THE AUDIT

As provided in the CPS.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCIES

As provided in the CPS.

8.6 COMMUNICATION OF RESULTS

As provided in the CPS.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 CERTIFICATE ISSUANCE AND RENEWAL FEES

The prices of certification services or any other related service are available and updated on Camerfirma's website https://www.camerfirma.com/certificados-digitales/ or after consultation with Camerfirma's support department at https://www.camerfirma.com/contacto-soporte/ or by calling +34 91 136 91 05.

Each type of certificate has a specific published retail price, except for those that are subject to prior commercial negotiation.

9.1.2 CERTIFICATE ACCESS FEES

As provided in the CPS.

9.1.3 REVOCATION OR STATUS INFORMATION ACCESS FEES

As provided in the CPS.

9.1.4 FEES FOR OTHER SERVICES

As provided in the CPS.

9.1.5 REFUND POLICY

As provided in the CPS.

9.2 FINANCIAL RESPONSIBILITY

9.2.1 INSURANCE COVERAGE

As provided in the CPS.

9.2.2 OTHER ASSETS

Not stipulated.

9.2.3 INSURANCE OR WARRANTY COVERAGE FOR END-ENTITIES

As provided in the CPS.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 SCOPE OF BUSINESS INFORMATION

As provided in the CPS.

9.3.2 INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION

As provided in the CPS.

9.3.3 RESPONSIBILITY TO PROTECT CONFIDENTIAL INFORMATION

As provided in the CPS.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 PRIVACY PLAN

As provided in the CPS.

9.4.2 INFORMATION TREATED AS PRIVATE

As provided in the CPS.

9.4.3 INFORMATION NOT DEEMED PRIVATE

As provided in the CPS.

9.4.4 RESPONSIBILITY TO PROTECT PRIVATE INFORMATION

As provided in the CPS.

9.4.5 NOTICE AND CONSENT TO USE PRIVATE INFORMATION

As provided in the CPS.

9.4.6 DISCLOSURE PURSUANT TO JUDICIAL OR ADMINISTRATIVE PROCESS

As provided in the CPS.

9.4.7 OTHER INFORMATION DISCLOSURE CIRCUMSTANCES

As provided in the CPS.

9.5 INTELLECTUAL PROPERTY RIGHTS

As provided in the CPS.

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 CA REPRESENTATIONS AND WARRANTIES

As provided in the CPS.

9.6.2 RA REPRESENTATIONS AND WARRANTIES

As provided in the CPS.

9.6.3 SUBSCRIBER REPRESENTATIONS AND WARRANTIES

As provided in the CPS.

9.6.4 RELYING PARTY REPRESENTATIONS AND WARRANTIES

As provided in the CPS.

9.6.5 REPRESENTATIONS AND WARRANTIES OF OTHER PARTICIPANTS

Not stipulated.

9.7 DISCLAIMER OF WARRANTIES

As provided in the CPS.

9.8 LIMITATION OF LIABILITY

As provided in the CPS.

9.9 INDEMNITIES

As provided in the CPS.

9.10 TERM AND TERMINATION

9.10.1 TERM

As provided in the CPS.

9.10.2 TERMINATION

As provided in the CPS.

9.10.3 EFFECT OF TERMINATION AND SURVIVAL

As provided in the CPS.

9.11 INDIVIDUAL NOTIFICATIONS AND COMMUNICATION WITH PARTICIPANTS

As provided in the CPS.

9.12 AMENDMENTS

9.12.1 PROCEDURE FOR AMENDMENTS

As provided in the CPS.

9.12.2 NOTIFICATION MECHANISM AND PERIOD

As provided in the CPS.

9.12.3 CIRCUMSTANCES IN WHICH OID MUST BE CHANGED

Not stipulated.

9.13 DISPUTE RESOLUTION PROCEDURE

As provided in the CPS.

9.14 GOVERNING LAW

As provided in the CPS.

9.15 COMPLIANCE WITH APPLICABLE LAW

As provided in the CPS.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 ENTIRE AGREEMENT

As provided in the CPS.

9.16.2 ASSIGNMENT

As provided in the CPS.

9.16.3 SEVERABILITY

As provided in the CPS.

9.16.4 ENFORCEMENT (ATTORNEY'S FEES WAIVERS OF RIGHTS)

As provided in the CPS.

9.16.5 FORCE MAJEURE

As provided in the CPS.

9.17 OTHER PROVISIONS

Not stipulated.

Apendice 1 History of the document

May 2025	V1.0	Document creation