Tinexta Infocert

CERTIFICATE POLICY
FOR NON-PERSONAL CERTIFICATES
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-2025-18-14

SELLO JURIDICO

Firmado digitalmente por SELLO JURIDICO
Fecha: 2025.05.29 15:45:54 +02'00'

INDEX

1 INTRODUCTION

1.1 OVERVIEW

The Certificate 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.

This CP establishes the requirements, rules and procedures applicable to the issuance, use, management and revocation of non-personal electronic certificates (electronic seal, code signing and OCSP) 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.

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

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

- **Qualified Certificate for Electronic Seal**:

  This qualified certificate identifies a legal entity (Subject / Creator of a Seal).

  The Applicant for this certificate must have powers of representation that allow him/her to request the certificate on behalf of the legal entity to which the certificate is issued.

  The use of the private key associated with this certificate provides integrity and authenticity to the documents and transactions to which it is applied.

  This certificate can be associated to a private key activated by a machine or application, to allow the operations that use it to be performed automatically and unassisted. It is also allowed as a machine or client application identification element in TLS secure electronic communication protocols.

  Camerfirma issues these qualified certificates in secure signature creation devices - QSCD (cryptographic smartcard or token) under OID 0.4.0.194112.1.3 according to ETSI EN 319 411-2 - QCP-l-qscd, and in non-QSCD devices under OID 0.4.0.194112.1.1 according to ETSI EN 319 411-2 - QCP-l.

- **Qualified Certificate for Seal for Public Administration**

  This qualified certificate identifies a legal entity of the Public Administration type (Subject / Creator of a Seal), in accordance with the provisions of Article 40 of Law 40/2015, of October 1, of the Public Sector Legal Regime.

  The Applicant for this certificate must have powers of representation that allow him/her to

request the certificate on behalf of the Public Administration to which the certificate is issued.

The use of the private key associated with this certificate provides integrity and authenticity to the documents and transactions to which it is applied.

This certificate can be associated to a private key activated by a machine or application, to allow the operations that use it to be performed automatically and unassisted. It is also allowed as a machine or client application identification element in TLS secure electronic communication protocols.

The certificates issued under these CPs can be used by signature systems for automated administrative action, in accordance with the provisions of Article 42 of Law 40/2015, of October 1, of the Public Sector Legal Regime.

The certificates issued under these CPs are in accordance with the national regulations of the Public Administration's electronic seal certificate profile established in section 9 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:

- at its high level: OID 2.16.724.1.3.5.6.1
- at its medium/substantial level: OID 2.16.724.1.3.5.6.2

Camerfirma issues these qualified certificates in secure signature creation devices - QSCD (cryptographic smartcard or token) under OID 0.4.0.194112.1.3 according to ETSI EN 319 411-2 - QCP-l-qscd, and in non-QSCD devices under OID 0.4.0.194112.1.1 according to ETSI EN 319 411-2 - QCP-l.

- **Code Signing Non-Qualified Certificate**

This non-qualified certificate identifies a legal entity (Subject / Creator of a Seal).

The Applicant for this certificate must have powers of representation that allow him/her to request the certificate on behalf of the legal entity to which the certificate is issued.

This certificate allows developers to apply a digital signature on code (ActiveX, java applets, macros for Microsoft Office, etc.), thus establishing integrity and authenticity guarantees on such code.

- **Non-Qualified Certificate for Electronic Seal**

This non-qualified certificate identifies a legal entity (Subject / Creator of a Seal).

The Applicant for this certificate must have powers of representation that allow him/her to request the certificate on behalf of the legal entity to which the certificate is issued.

The use of the private key associated with this certificate provides integrity and authenticity to the documents and transactions to which it is applied.

This certificate can be associated to a private key activated by a machine or application, to allow the operations that use it to be performed automatically and unassisted. It is also allowed as a machine or client application identification element in TLS secure electronic communication protocols.

- **Non-Qualified Certificate for Electronic Seal for Public Administration**

  This non-qualfiied certificate identifies a legal entity of the Public Administration type (Subject / Creator of a Seal).

  The Applicant for this certificate must have powers of representation that allow him/her to request the certificate on behalf of the legal entity to which the certificate is issued.

  The use of the private key associated with this certificate provides integrity and authenticity to the documents and transactions to which it is applied.

  This certificate can be associated to a private key activated by a machine or application, to allow the operations that use it to be performed automatically and unassisted. It is also allowed as a machine or client application identification element in TLS secure electronic communication protocols.

- **Non-Qualified OCSP Certificate**

  Each Root CA and each SubCA managed by Camerfirma within the hierarchies under this CPS issues an OCSP certificate, under the corresponding "CP Non-Qualified OCSP Certificate", which will be used to sign the responses of the CA's OCSP service about the status of the certificates issued by the CA, while the CA is active.

- **TSU Qualified Certificate QSCD**

  This qualified certificate identifies a legal person (Subject / Creator of a Seal).

  The Applicant for this certificate must have powers of representation that enable him/her to apply for the certificate on behalf of the legal person to which the certificate is issued.

  This certificate can be used for digital signing of time-stamps.

  The keys of this certificate are generated and stored in an HSM QSCD, in accordance with t he requirements set out in ETSI EN 319 421.

1.2 IDENTIFICATION AND NAME OF THE DOCUMENT

Name:	Certificate Policy for CAMERFIRMA's NON-personal Certificates
Description:	Certification Policies for CAMERFIRMA's NON-personal certificates: electronic seal

	certificates, code signing certificates and OCSP certificates.
Version:	See home page
OID:	• **Qualified Certificate for Electronic Seal** CHAMBERS OF COMMERCE ROOT Hierarchy - 2016 AC CAMERFIRMA FOR LEGAL PERSONS - 2016 ○ 1.3.6.1.4.1.17326.10.16.2.1.1 QSCD SmartCard/Token ○ 1.3.6.1.4.1.1.17326.10.16.2.1.2 Non QSCD ○ 1.3.6.1.4.1.17326.10.16.2.1.3 Authentication ○ 1.3.6.1.4.1.17326.10.16.2.1.4 Signature • **Qualified Certificate for Electronic Seal for Public Administrations** CHAMBERS OF COMMERCE ROOT Hierarchy - 2016 AC CAMERFIRMA FOR LEGAL PERSONS - 2016 ○ 1.3.6.1.4.1.17326.10.16.2.2.2.1.3.3.3.1 High Level QSCD SmartCard/Token ○ 1.3.6.1.4.1.17326.10.16.2.2.2.1.4.3.1 Medium level - Non QSCD Hierarchy CHAMBERS OF COMMERCE ROOT - 2008 Camerfirma AAPP II - 2014 ○ 1.3.6.1.4.1.1.17326.1.3.3.2 (no new certificates are issued) • **CP TSU Qualified Certificate** CHAMBERS OF COMMERCE ROOT – 2016 hierarchy AC CAMERFIRMA TSA - 2016 ○ 1.3.6.1.4.1.17326.10.16.5.1.1 - QSCD HSM (no new certificates are issued) INFOCERT-CAMERFIRMA TIMESTAMP 2024 INFOCERT-CAMERFIRMA QUALIFIED TSA - 2024 ○ 1.3.6.1.4.1.17326.10.21.30.4 - QSCD HSM • **Code Signing Non-Qualified Certificates** Hierarchy CHAMBERS OF COMMERCE ROOT - 2008 Camerfirma Codesign II - 2014 ○ 1.3.6.1.4.1.17326.10.12.2 • **Non-Qualified Certificate for Electronic Seal** Hierarchy CHAMBERS OF COMMERCE ROOT - 2008 Camerfirma Corporate Server II - 2015 ○ 1.3.6.1.4.1.17326.10.11.3.1.1 (P12) ○ 1.3.6.1.4.1.17326.10.11.3.1.2 (CSR) Camerfirma AAPP II - 2014 (no new certificates are issued) ○ 1.3.6.1.4.1.17326.1.3.3.2 • **Non-Qualified OCSP Certificates** Hierarchies Chambers of Commerce Root - 2008, CHAMBERS OF COMMERCE ROOT - 2016 GLOBAL CHAMBERSIGN ROOT - 2016 ○ 1.3.6.1.4.1.17326.10.9.8 (HSM) CAMERFIRMA ROOT 2021 Hierarchy ○ 1.3.6.1.4.1.17326.10.21.0.1 (HSM)
Location:	https://www.camerfirma.com/practicas-de-certificacion-ac-camerfirma-CPS-CPS/

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

1.3 PKI PARTICIPANTS

1.3.1 CERTIFICATION AUTHORITIES (CA)

Under this CP, Camerfirma manages the following CA hierarchies:

- CHAMBERS OF COMMERCE ROOT 2016:
  - AC CAMERFIRMA FOR LEGAL PERSONS - 2016
  - AC CAMERFIRMA TSA - 2016
- CHAMBERS OF COMMERCE ROOT 2008:
  - Camerfirma Codesign II - 2014
  - Camerfirma Corporate Server II - 2015
  - Camerfirma AAPP II - 2014
- CAMERFIRMA ROOT 2021:
  - AC CAMERFIRMA QUALIFIED CERTIFICATES - 2021
- INFOCERT-CAMERFIRMA TIMESTAMP - 2024
  - INFOCERT-CAMERFIRMA QUALIFIED TSA - 2024

1.3.1.1 TEST CERTIFICATES

As provided in the CPS.

1.3.2 REGISTRATION AUTHORITIES (RA)

The following types of RA are recognized under this CP:

- Cameral RA: 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 RA: 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 Subordinated 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 demarcation, unless otherwise determined by the CA.

  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 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 prepared 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 does not have 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 delegated by the RA to the PVR.

1.3.3 SUBSCRIBERS

1.3.3.1 SUBSCRIBER

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

- The Entity (legal entity) Subject.
- The Entity (legal entity) identified in the certificate to which the Subject is linked, in cases where the Subject is not the Entity.
- A legal person with powers of representation of the Entity (legal person) Subject.
- A legal person with powers of representation of the Entity (legal person) identified in the certificate to which the Subject is bound, in cases where the Subject is not the Entity.

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

- A third organization acting as RA under this CPS and as Underwriter 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:

- The Entity (legal entity) to which the certificate is issued. The Subscriber is the Subject Entity (the legal person identified in the certificate) or another legal person empowered to represent the Subject Entity.
- An organization, unit, area or department linked to the Entity (legal entity) to which the certificate is issued. The Subscriber is the Entity identified in the certificate to which the Registrant is bound (the legal person identified in the certificate) or another legal person with powers of representation of the Entity identified in the certificate to which the Registrant is bound.
- A device, application or system operated by or on behalf of the Entity (legal entity) to which the certificate is issued. The Subscriber is the Entity identified in the certificate to which the Certificate Subject (the legal entity identified in the certificate) or another legal entity with authority to represent the Entity identified in the certificate to which the Certificate Subject is bound is bound.

Under this CP, and in accordance with the eIDAS Regulation, the **Creator of a Seal** is the legal entity identified in an electronic seal certificate, which may be:

- If the Subject is the Entity (legal entity) to which the certificate is issued, the Creator of a Seal is the Entity (legal entity), the Subject and, if applicable, the Subscriber.
- If the Subject is an organization, unit, area or department linked to the Entity (legal person) to which the certificate is issued, the Creator of a Seal is the Entity (legal person) to which the Subject is linked and, if applicable, the Subscriber.
- If the Subject is a device, application or system operated by or on behalf of the Entity (legal entity) to which the certificate is issued, the Creator of a Seal is the Entity (legal entity) to which the Subject and, if applicable, the Subscriber is linked.

The Creator of a Seal, as a legal person Subject of the electronic seal certificate, or as a legal person to which the Subject of the electronic seal certificate is linked, shall be directly responsible for the obligations associated with the use and management of the certificate and its associated private key, without prejudice to the obligations of the Controller and, if applicable, of the Subject.

1.3.3.3 APPLICANT

Under these CPs, the Applicant for a certificate shall be the natural person requesting a certificate for the legal entity he/she represents.

Under these CPs, the certificate Applicant may be a natural person with powers of representation that allow him/her to request the certificate on behalf of the Entity (legal entity) to which the certificate is issued.

1.3.3.4 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 Creator of a Seal and, if applicable, of the Subject.

1.3.3.5 ENTITY

Under this CP, the Entity is, if applicable, the organization, public or private, individual or collective, recognized in law, identified in the *organizationName* (O) and *organizationIdentifier* attributes of the *subject* field of a certificate, with which the Subject has a certain relationship, or which identifies the Subject.

Under these CPs, the Entity of a certificate may be the legal entity identified in the certificate, which may be:

- If the Subject is the Entity (legal entity) to which the certificate is issued, the Subject, Subscriber and Creator of a Seal.
- If the Subject is an organization, unit, area or department linked to the Entity (legal entity) to which the certificate is issued, the Subscriber and Creator of a Seal.
- If the Subject is a device, application or system operated by or on behalf of the Entity (legal entity) to which the certificate is issued, the Subscriber and Creator of a Seal.

1.3.4 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.

1.3.5 OTHER PARTICIPANTS

1.3.5.1 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.
- Advanced electronic seal, or qualified electronic seal when used with qualified electronic seal creation devices.

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 CPS, 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-CPS/
- 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 legal entities, except for TSU and OCSP certificates:
    - If the Subject is the Entity (legal entity) to which the certificate is issued:
        - Company name and fiscal identifier of the Entity.
        - Country where the legal entity owner carries out the activity (C).
    - If the Subject is an organization, unit, area or department linked to the Entity (legal entity) to which the certificate is issued:
        - Company name and fiscal identifier of the Entity.
        - Unit, area or department.
        - Country where the legal entity owner carries out the activity (C).
    - If the Subject is a device, application or system operated by or on behalf of the Entity (legal entity) to which the certificate is issued:
        - Company name and fiscal identifier of the Entity.
        - Name of the device, application or system.
        - Country where the legal entity owner carries out the activity (C).
- For CA, TSU and OCSP certificates (issued to legal entities), in the DN in the *Subject* field:
    - Descriptive name of the CA, TSU or OCSP service (*CN*).
    - Corporate name of the legal entity owner (O).
    - Fiscal identifier of the owning legal entity (*organizationIdentifier* and/or *serialNumber*).
    - Country where the legal entity owner carries out the activity (C).

The certificate profile files under these CPS and 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

These types of certificates do not accept pseudonyms of the subscribers.

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

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, as long as they contain the applicant's identity data.

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 Applicant's identity or other permanent circumstances 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 unqualified 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.

3.2.1 METHODS OF PROOF OF POSSESSION OF THE PRIVATE KEY

As provided in the CPS

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 Certificate for Electronic Seal	In case that the Applicant and the Responsible are different persons, authorization signed by the Applicant (authorizing) to the Responsible

	(authorized), to request and be delivered the certificate and make use of it. Certificate or consultation of the Commercial Registry to verify the incorporation and legal personality of the Entity, and the appointment and validity of the position of the Applicant (if applicable, at the same time, authorizer) with powers of representation that allow him/her to request the certificate on behalf of the Entity (legal person).
Qualified Certificate for Electronic Seal for Public Administrations	In case that the Applicant and the Responsible are different persons, authorization signed by the Applicant (authorizing) to the Responsible (authorized), to request and be delivered the certificate and make use of it. Certificate to prove the appointment and validity of the position of the Applicant (if applicable, at the same time, authorizer) with powers of representation that allow him/her to request the certificate on behalf of the Entity (legal entity), or appointment of the Applicant in the Official Gazette where the DNI/NIE of this person is stated.
TSU Qualified Certificate Non-Qualified Code Signing Certificate	In case that the Applicant and the Responsible are different persons, authorization signed by the Applicant (authorizing) to the Responsible (authorized), to request and be delivered the certificate and make use of it. In case that the Entity is not a Public Administration, certificate or consultation to the Commercial Registry to verify the constitution and legal personality of the Entity, and the appointment and validity of the Applicant position (in its case, at the same time, of the authorizer) with powers of representation that allow him/her to request the certificate on behalf of the Entity (legal person). In case that the Entity is a Public Administration, certificate to verify the appointment and validity of the position of the

	Applicant (if applicable, at the same time, authorizer) with powers of representation that allow him/her to request the certificate on behalf of the Entity (legal entity), or appointment of the Applicant in the Official Gazette where the DNI/NIE of this person is stated.
Non-Qualified Certificate for Electronic Seal	In case that the Applicant and the Responsible are different persons, authorization signed by the Applicant (authorizing) to the Responsible (authorized), to request and be delivered the certificate and make use of it. Certificate to prove the appointment and validity of the position of the Applicant (if applicable, at the same time, authorizer) with powers of representation that allow him/her to request the certificate on behalf of the Entity (legal entity), or appointment of the Applicant in the Official Gazette where the DNI/NIE of this person is stated.
Non-Qualified Certificate for Electronic Seal for Public Administrations	In case the Applicant and the Person Responsible are different persons, authorization signed by the Applicant (authorizing person) to the Person Responsible(authorized person), to request and be given the certificate and make use of it. Certificate to verify appointment and validity of the position of the Applicant (if applicable, at the same time, authorizing person) with powers of representation that allow him/her to apply for the certificate on behalf of the Entity (legal person), or appointment in the Official State Gazette where this person's DNI/NIE No. appears.

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 Party is notified by e-mail of 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

As provided in the CPS

4.5 KEY PAIR AND CERTIFICATE USAGE

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*.

CA/PC	Key Usage	Extended Key Usage	Basic Constraints
CHAMBERS OF COMMERCE ROOT - 2016	critical, cRLSign, keyCertSign	-	critical, CA:true
AC CAMERFIRMA FOR LEGAL PERSONS - 2016	critical, cRLSign, keyCertSign	emailProtection clientAuth	critical, CA:true, pathLen:2
Qualified Certificate for Electronic Seal - QSCD SmarSmartCard/Token, Non QSCD	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical, CA:false
AAPP Qualified Certificate of Electronic Seal - High Level - QSCD SmartCard/Token	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical, CA:false
Qualified Certificate of Electronic Seal AAPP - Intermediate Level - No QSCD	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical, CA:false
Qualified Certificate of Electronic Stamp Authentication	digitalSignature	clientAuth	
Qualified Certificate of Electronic	nonRepudiation	-	critical, CA:false

Seal Signature			
Chambers of Commerce Root - 2008 (SHA-1 certificate)	critical, cRLSign, keyCertSign	-	critical, CA:true, pathLen:12
Chambers of Commerce Root - 2008 (certificate SHA -256)	critical, cRLSign, keyCertSign	-	critical, CA:true, pathLen:12
Camerfirma Codesign II - 2014	critical, cRLSign, keyCertSign	codesigning msCodeCom	critical, CA:true, pathLen:2
Code Signing Non-Qualified Certificate	critical, digitalSignature, nonRepudiation	codesigning msCodeCom	critical, CA:false
Camerfirma Corporate Server II - 2015	critical, cRLSign, keyCertSign	emailProtection clientAuth serverAuth	critical, CA:true, pathLen:2
Non-Qualified Certificate for Electronic Seal - P12, P10	critical, digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement	clientAuth emailProtection	critical, CA:false
Camerfirma AAPP II - 2014	critical, cRLSign, keyCertSign	emailProtection clientAuth serverAuth	critical, CA:true, pathLen:2
Non-Qualified Certificate for Electronic Seal for Public Administration	critical, digitalSignature, contentCommitment, keyEncipherment, dataEncipherment	clientAuth emailProtection	critical, CA:false
GLOBAL CHAMBERSIGN ROOT - 2016	critical, cRLSign, keyCertSign	-	critical, CA:true
AC CAMERFIRMA COLOMBIA - 2016	critical, cRLSign, keyCertSign	-	critical, CA:true, pathLen:2
AC CAMERFIRMA PERU - 2016	critical, cRLSign, keyCertSign	-	critical, CA:true, pathLen:2
CAMERFIRMA ROOT 2021	critical, cRLSign, keyCertSign	-	critical, CA:true
AC CAMERFIRMA QUALIFIED CERTIFICATES - 2021	critical, cRLSign, keyCertSign	emailProtection, clientAuth	critical, CA:true, pathLen:0

Non-Qualified OCSP Certificate - HSM	critical, digitalSignature, nonRepudiation	OCSPSigning	critical, CA:false
INFOCERT-CAMERFIRMA TIMESTAMP 2024	critical, cRLSign, keyCertSign	-	critical, CA:true
INFOCERT-CAMERFIRMA QUALIFIED TSA - 2024	critical, cRLSign, keyCertSign	emailProtection, clientAuth	critical, CA:true, pathLen:0
TSU Qualified Certificate - QSCD HSM	critical, contentCommitment,	timeStamping	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 seal certificates, the Subject / Creator of a Seal must keep the remote seal authentication tools and/or devices secure. He must also keep the remote seal certificate's private key activation PIN under his control and separate from the authentication passwords or authentication devices. Finally, you must ensure that the privacy and preservation of the certificate revocation PIN is maintained. The Subject / Creator of a Seal must not create digital seals 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 case of a qualified certificate, more than 5 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

According to the provisions of the CPS

4.7.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RE-KEY CERTIFICATE

In accordance with the provisions of the CPS

4.7.6 PUBLICATION OF THE RE-KEYED CERTIFICATE BY THE CA

According to the provisions of 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 CRLS

As provided in the CPS.

4.9.9 ON-LINE REVOCATION/STATUS CHECKING AVAILABILITY

According to the provisions of the CPS

4.9.10 ON-LINE REVOCATION CHECKING REQUIREMENTS

According to the provisions of 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 PREVENTION AND PROTECTION

As provided in the CPS.

5.1.6 MEDIA STORAGE

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 CERTIFICATE 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.

Apendix 1 Document History

May 2025	V1.0	Document creation