# CERTIFICATION PRACTICES STATEMENT DIGITAL CERTIFICATES AC CAMERFIRMA SA EIDAS-2016

**CHAMBERS OF COMMERCE ROOT - 2016**
**CHAMBERS OF COMMERCE ROOT - 2018** and
**GLOBAL CHAMBERSIGN ROOT - 2016**.

Version 1.2.4

**Author:** Juan Ángel Martín: PKI Area.
Luis Miguel Aldea and Eva Vaquero: Systems Area.
Laura Montoya: Legal Area.
Raquel Rodríguez: Operations Area.

**Revised by:** Ramiro Muñoz Muñoz (Operations Management).
**Approved by (PA):** Rosario Márquez (Corporate Management).
**Auditor:** Auren España.

Document valid only in digital format digitally signed by the Policy Authority.
This document can be obtained from the website address https://policy.camerfirma.com/ or by email juridico@camerfirma.com

Language: English

| | | |
|---|---|---|
| May 2016 | V1.0 | eIDAS adaptation |
| Nov 2016 | V1.1 | Modifications made to the conformity evaluation process. |
| March 2017 | V1.2 | Expansion of CA structures, reviewing and modifying certificate profiles. |
| April 2017 | V1.2.1 | Incorporation of CAA checks into Secure Server and Digital Office certificates pursuant to RFC 6844. |
| February 2018 | V1.2.2 | 1.2 clarification on the alignment of these practices with the Baseline Requirements of CA-B FORUM (point 1.1 after adaptation to structure RFC3647)<br>1.2.1.3 - OIDs corrections of EP certificates with PSEUDÓNIMO (point 1.3.11.3 after adaptation to structure RFC3647)<br>1.2.1.3.4 - Clarification of the duration of the TSU certificates and acceptance of the practices by the subscriber with an approved TSU device. (point 1.3.11.3.4 after adaptation to structure RFC3647)<br>1.2.1.4.3 - Incorporation of the date of deployment of Camerfirma Peru (point 1.3.11.4.1.7 after adaptation to structure RFC3647)<br>1.5.5 - Incorporation of the figure of Delegate Agency for Camerfirma Peru (point 1.3.2 after adaptation to structure RFC3647)<br>4.8.3 Revocation by third parties. Revocation in case of an incorrect issuance (CABFORUM requirement). (point 4.9.2 after adaptation to structure RFC3647) |
| March 2018 | V1.2.3 | 1.5.5 RAs for SSL can't validate the domain. CA / B Forum. (point 1.3.2 after adaptation to structure RFC3647)<br>2.5.3 Clarification free service OCSP. (point 9.1.3 after adaptation to structure RFC3647)<br>2.1.5 user responsibility - TSL check (point 9.6.4 after adaptation to structure RFC3647) |
| May 2018 | V1.2.4 | Clarifications concepts Subject / Holder and Signer / Creator of the seal.<br>Adaptation of the structure of the CPD document based on RFC3647<br>Incorporation of hierarchy CHAMBERS OF COMMERCE ROOT - 2018<br>Incorporation of subordinated CA AC CAMERFIRMA GLOBAL TSA - 2018 |

# Table of Contents

# 1 Introduction

## *1.1 General Overview*

Given that there is no specific definition of the concepts of the Certification Practices and Certification Policies Statement, and due to some confusion that has arisen, Camerfirma would like to explain its stance in relation to these concepts.

**Certification Policy (CP)**: a set of rules defining the applicability of a certificate in a community and/or in an application, with common security and usage requirements. In other words, a Certification Policy must generally define the applicability of certificate types for certain applications that establish the same security and usage requirements.

**Certification Practices Statement (CPS)**: defined as a set of practices adopted by a Certification Authority for the issuance of certificates. It usually contains detailed information about its certificate security, support, administration and issuing system, as well as the trust relationship between the Subject/Signatory, the User Party and the Certification Authority. These may be completely comprehensible and robust documents that provide an accurate description of the services offered, detailed certificate lifecycle management procedures, etc.

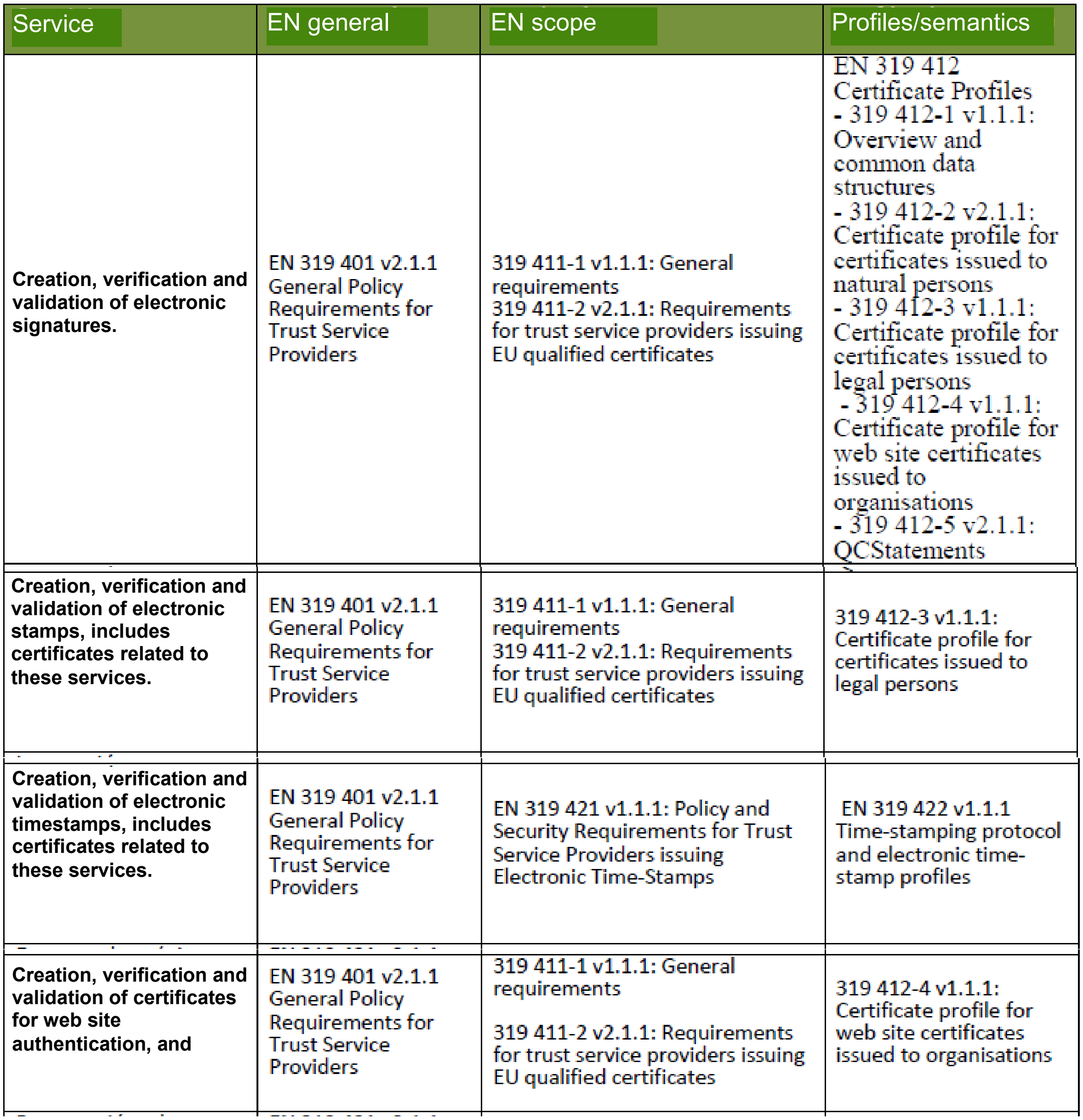
These Certification Policies and Certification Practices Statement concepts are different, although they are still closely interrelated.

A detailed Certification Practices Statement is not an acceptable basis for the interoperability of Certification Authorities. On the whole, Certification Policies are a better basis for common security standards and criteria.

In summary, a Policy defines “which” security requirements are required for the issuance of certificates. The Certification Practices Statement defines **“how”** the security requirements established in the Policy are fulfilled.

Regulation (EU) 910/2014 of the European Parliament and Council, 23 July 2014, about digital identification and trust services for digital transactions in the internal market and amending Directive 1999/93/CE (hereinafter, eIDAS), establishes that trusted services include the following digital services normally provided in exchange for remuneration: - The creation, verification and validation of digital signatures. Certificates relating to these services are included: - the creation, verification and validation of digital seals. Certificates relating to these services are included: - the creation, verification and validation of digital timestamps. Certificates relating to these services are included: certified digital delivery. Certificates relating to these services are included: - the creation, verification and validation of certificates for authentication of websites, and - the preservation of digital signatures, stamps or certificates for these services.

This document specifies the Certification Practices Statement (hereinafter, CPS) that AC Camerfirma SA (hereinafter, Camerfirma) has established for issuing trusted certificates and services based on the following standards:



| Service | EN general | EN scope | Profiles/semantics |
|---|---|---|---|
| **Creation, verification and validation of electronic signatures.** | EN 319 401 v2.1.1 General Policy Requirements for Trust Service Providers | 319 411-1 v1.1.1: General requirements<br>319 411-2 v2.1.1: Requirements for trust service providers issuing EU qualified certificates | EN 319 412 Certificate Profiles<br>- 319 412-1 v1.1.1: Overview and common data structures<br>- 319 412-2 v2.1.1: Certificate profile for certificates issued to natural persons<br>- 319 412-3 v1.1.1: Certificate profile for certificates issued to legal persons<br>- 319 412-4 v1.1.1: Certificate profile for web site certificates issued to organisations<br>- 319 412-5 v2.1.1: QCStatements |
| **Creation, verification and validation of electronic stamps, includes certificates related to these services.** | EN 319 401 v2.1.1 General Policy Requirements for Trust Service Providers | 319 411-1 v1.1.1: General requirements<br>319 411-2 v2.1.1: Requirements for trust service providers issuing EU qualified certificates | 319 412-3 v1.1.1: Certificate profile for certificates issued to legal persons |
| **Creation, verification and validation of electronic timestamps, includes certificates related to these services.** | EN 319 401 v2.1.1 General Policy Requirements for Trust Service Providers | EN 319 421 v1.1.1: Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps | EN 319 422 v1.1.1 Time-stamping protocol and electronic time-stamp profiles |
| **Creation, verification and validation of certificates for web site authentication, and** | EN 319 401 v2.1.1 General Policy Requirements for Trust Service Providers | 319 411-1 v1.1.1: General requirements<br>319 411-2 v2.1.1: Requirements for trust service providers issuing EU qualified certificates | 319 412-4 v1.1.1: Certificate profile for web site certificates issued to organisations |

Regarding the policies to be applied in accordance with EN 319 411-1 / 2, the following policy groups are described:

**General policies:**

- **NCP** Standardised certification policy.
- **NCP+** Standardised certification policy with secure device.
- **LCP** Light certification policy (without physical presence).
- **EVCP** Certificate policy for extended validation certificates.
- **DVCP** Certificate policy for domain validation certificates.
- **OVCP** Certificate policy for organisation validation certificates.

**Policies for qualified certificates:**

- **QCP-n** Policies for qualified certificates issued to natural persons. Includes the **NCP** policy requirements plus additional requirements to support the management of qualified certificates.
- **QCP-l** Policies for qualified certificates issued to legal entities. Includes the **NCP** policy requirements plus additional requirements to support the management of qualified certificates.
- **QCP-n-qscd** Policies for qualified certificates issued to natural persons with SSCD. Includes the **QCP-n (including NCP+**) policy requirements plus additional requirements to support the management of qualified certificates and the provision of secure signature creation devices.
- **QCP-l-qscd** Policies for qualified certificates issued to natural persons with SSCD. Includes the **QCP-l** (including **NCP+**) policy requirements plus additional requirements to support the management of qualified certificates and the provision of secure signature creation devices.
- **QCP-w** Policies for qualified certificates issued to web servers. When the certificate is issued to a legal entity the **EVCP** policy requirements plus additional requirements to support the management of qualified certificates. When the certificate is issued to a natural person it includes the **NCP** policy requirements plus additional requirements to support the management of qualified certificates.

Additionally in the requirements established in the certification policies to which this CPS refers. The recommendations in the technical document *Security CWA 14167-1 Requirements for Trustworthy Systems Managing Certificates for Digital Signatures - Part 1: System Security Requirements.*

**These practices are aligned with the requirements established in the Baseline Requirements for the Issue and Management of Publicly-Trusted Certificates from the CA / BROWSER FORUM http://www.cabforum.org in its version 1.5.4.**

This CPS is compliant with the Certification Policies for the different certificates that Camerfirma issues, which are described in section 1.3.11 of this CPS. In the event of any conflict between both documents, the provisions of this document shall prevail.

## 1.2 Document Name and Identification

| | |
|---|---|
| **Name:** | CPS Camerfirma SA. |
| **Description:** | A document that responds to the requirements of the Policies described and identified in the previous points of this document describing the hierarchies affected. |
| **Version:** | See homepage |
| **OID** | 1.3.6.1.4.1.17326.10.1 |
| **Location:** | https://policy.camerfirma.com/ |

## 1.3 Community and Scope of Application.

### 1.3.1 Certification Authority (CA).

The component of a PKI responsible for issuing and managing digital certificates. It acts as the trusted third party between the Subject (Signatory) and the User Party in digital transactions, associating a specific public key with a person. The CA has the ultimate responsibility in the provision of certification services. The CA is identified in the Subject (Issuer) field of the digital certificate.

A CA is a type of Trusted Service Provider (TSP) that issues digital certificates.

A TSP can incorporate a CA hierarchy. This CA hierarchy is associated with a root CA. The TSP is responsible for ensuring all the CAs included in the hierarchy meet the requirements of the corresponding policies. There may be more than one intermediate CA between the root certification authority and the final-entity certificate. The number of intermediate CAs allowed is specified in the Basic Constraints (pathLenConstraint) extension of the Certification Authority's certificate.

A Certification Authority (CA) uses Registration Authorities (RA) for the purpose of testing and storage of digital certificate content documentation. The CAs can carry out the RAs' work at any time.

A CA belongs to a legal entity specified in the organisation attribute (O) of the issuer field (*Issuer*) of the associated digital certificate.

Information related to the CAs managed by Camerfirma can be found in this document or on Camerfirma's website http://www.camerfirma.com.

### 1.3.2 Registration Authority (RA)

An RA may be a natural person or a legal entity acting in accordance with this CPS and, if applicable, through an agreement with a specific CA, exercising the roles of managing the requests, identification and registration of certificate applicants, and any responsibilities established in the specific Certification Policies. RAs are authorities delegated by the CA, although the latter is ultimately responsible for the service.

Under current practices, the following types of RA are recognised:

- **Chambers RA:** Those managed directly or under the control of a Spanish Chamber of Commerce, Industry and Navigation.
- **Corporate RA:** Managed by a public organisation or a private entity for distributing certificates to its employees.
- **Remote RA:** A registration authority managed in a remote location that communicates with the platform through the AC Camerfirma - STATUS management platform integration layer.

For the purpose of this CPS, the following can act as RAs:

- ❑ The Certification Authority.
- ❑ The Spanish Chambers of Commerce, Industry and Navigation, or the entities appointed by them. The delegated entities can carry out the registration process.
- ❑ Spanish Company Registration Authorities (Company RA), as entities delegated by an RA, to which they are contractually associated, in order to make the complete records of Subjects/Signatories within a particular organisation or demarcation. In general, the operators of these RA companies only manage the applications and certificates in the area of their organisation or demarcation, unless determined otherwise by the RA on which they depend. For example, a corporation's employees, members of a corporate group, members of a professional body.
- ❑ Entities belonging to the Spanish public administrations.
- ❑ Other Spanish or international agents that have a contractual relationship with the CA and have passed the registration processes. They are obliged to pass the audits required in the corresponding Certification Policies.

**In the issuance of Secure Server certificates the delegation of domain validation to an external RA IS NOT allowed in any case.**

| CHAMBERS OF COMMERCE ROOT | AC | Cámaras Comercio españolas | Empresa española | Administraciones Publicas española | Otros |
|---|---|---|---|---|---|
| AC CAMERFIRMA FOR NATURAL PERSONS | yes | yes | yes | yes | no |
| AC CAMERFIRMA FOR LEGAL PERSONS | yes | yes | yes | yes | no |
| AC CAMERFIRMA FOR WEBSITES | yes | no | yes | no | no |
| AC CAMERFIRMA CODESIGN | yes | no | No | no | no |
| AC CAMERFIRMA TSA | yes | no | No | no | no |
| GLOBAL CHAMBERSIGN ROOT | yes | | | | |
| AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS | yes | yes | yes | yes | yes |
| AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS | yes | yes | yes | yes | yes |

| | | | | | |
|---|---|---|---|---|---|
| AC CAMERFIRMA GLOBAL FOR WEBSITES | yes | no | no | no | no |
| AC CAMERFIRMA GLOBAL TSA | yes | no | no | no | yes |

- **PVP.** Point of Physical Verification that always depends on an RA. Its main mission is to provide evidence of the applicant's physical presence and deliver the documentation to the RA, which is validated in accordance with applicable policy for processing the application for issuing the certificate. For these functions, the PVPs are not subject to training or controls.

  Sometimes, the PVPs' functions may be extended to compiling the documentation submitted, checking its suitability for the type of certificate requested and delivery to the applicant in the case of the cryptographic card. AC Camerfirma has drafted a relationship type document between the RA and the PVP.

  Given that they do not have the capacity to register, they are contractually linked to an RA through a standard contract provided by Camerfirma. Based on the documentation provided by the PVP, the operator of the RA checks the documentation, and if applicable, gives course to the issuance of the certificate by the CA without having to make another face-to-face verification. The contract defines the functions delegated by the RA in the PVP.

- **Delegate Agency.** (only applicable for AC CAMERFIRMA PERU): the RAs can delegate by contract, to trust entities, the same functions that they are assuming as RA duly accredited, in order to offer the same service in geographical areas far from the RA's address. Although they are generally entities with legal personality different from that of the RA, in their capacity as Delegated Agency of the RA, they will be subject to control and follow-up as if it were a branch of the RA, having to assume the same obligations and responsibilities and submit in its case, to the audits carried out to the RA by the competent oversight body.

  The Delegate Agency must have the necessary capacity to determine the identity, capacity and freedom of action of the applicants. Their intervention will be carried out with the physical presence of the applicant, collating original documents with the copies provided by the user, or with information included in the processing forms. At any time, the RE may perform internal audits to verify the correct performance of the functions.

  The ER will assess the adequacy of the Delegate Agency's capacity based on its prestige, independence and prior relationship it may have with the users and must communicate its creation to the supervisory body.

| CHAMBERS OF COMMERCE ROOT - 2016 | CA | Spanish Chambers of Commerce | Spanish company | Spanish Public Administrations | Other |
|---|---|---|---|---|---|
| AC CAMERFIRMA FOR NATURAL PERSONS | yes | yes | yes | yes | no |
| AC CAMERFIRMA FOR LEGAL PERSONS | yes | yes | yes | yes | no |

| | | | | | |
|---|---|---|---|---|---|
| AC CAMERFIRMA FOR WEBSITES | yes | no | yes | no | no |
| AC CAMERFIRMA CODESIGN | yes | no | no | no | no |
| AC CAMERFIRMA TSA | yes | no | no | no | no |
| GLOBAL CHAMBERSIGN ROOT - 2016 | | | | | |
| AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS | yes | yes | yes | yes | yes |
| AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS | yes | yes | yes | yes | yes |
| AC CAMERFIRMA GLOBAL WEBSITES | yes | no | no | no | no |
| AC CAMERFIRMA GLOBAL TSA | yes | no | no | no | yes |

### 1.3.3 Subject/Certificate holder and Signatory.

The *'Subject'* is the certificate holder and is described in the CN (*Common Name*) attribute of the DN (*Distinguished Name*) field of the certificate. The Subject may be:

- ❑ A natural person.
- ❑ A natural person associated with an organisation.
- ❑ A legal entity.
- ❑ A hardware device or software application operated by or on behalf of a legal entity.

When a Signatory is the Subject of the certificate, the Signatory is directly responsible for the obligations associated with managing the certificate.

When a Signatory acts on behalf of one or more Subjects to which the Signatory is associated (example: a company that requests certificates for its employees to act on behalf of the company).

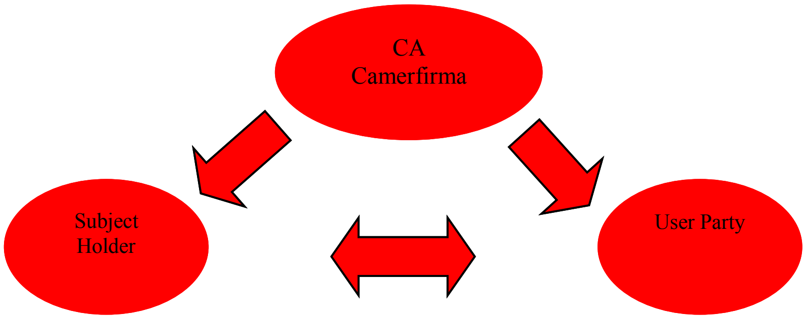
The connections between the Subject and the Signatory may be:

- ❑ When it is a natural person the Signatory may be:
  - o The natural person
  - o A natural person representing the certificate's Subject.
  - o Any entity authorised to represent the legal entity for which the entity is identified in association with the certificate's organisation field (O).
- ❑ When it is a legal entity, the Creator of the Seal may be:
  - o Any entity authorised to represent the legal entity.
  - o A legal representative.
- ❑ When it is a device, the Signatory may be:
  - o The natural person operating the device or application.
  - o Any entity authorised to represent the legal entity.
  - o A legal representative.

In order to avoid a conflict of interest, AC Camerfirma does not allow the Signatory and RA to be the same entity except when requesting certificates for an organisation associated with the RA or people associated with this organisation.

### 1.3.4 User Party or certificate user.

In this CPS, the User Party or user is the person receiving a digital transaction carried out with a certificate issued by any of the Camerfirma CAs and who voluntarily trusts the Certificate that this CA issues. Flow diagram.



### 1.3.5 Intermediate or Subordinate Certification Authority.

An Intermediate Certification Authority or Subordinate CA is a hierarchical object that obtains a certificate from the Root CA to issue final-entity certificates or other CA certificates.

The Subordinate CAs enable risks to be distributed in a complex hierarchical structure, which allows their keys to be managed in a more agile "online" environment, protecting the CA Root keys stored in a secure disconnected environment. A Subordinate CA enables the organisation of various types of certificates issued by the main CA.

The Subordinate CA's certificate is signed by a root CA certificate (origin root entity of the certification hierarchy) or another Subordinate CA.

A Subordinate CA may be subject to limitations by the CA on which it depends hierarchically:

a) Technically by a combination of the following parameters within the certificate: *Extended Key Usage* and *Name Constraints*
b) Contractually.

An intermediate Authority can be identified as internal or external. An **Internal Subordinate CA** is owned by the same organisation as the CA on which it depends hierarchically, in this case, AC Camerfirma. By contrast, an **external Subordinate CA** is owned by a different organisation, which has applied to join the hierarchy of the CA on which it depends hierarchically and may or may not use a different technical infrastructure employed by it.

### 1.3.6 Accreditation Entity or Supervisory Body.

The supervision authority is the corresponding management entity that accepts, accredits and supervises the TSPs within a specific geographic area. Within Spain, this task is the responsibility of the Ministry for Energy, Tourism and the Digital Agenda, which is the competent authority depending on the Spanish State member of the European Economic Space.

The Subordinate CAs that Camerfirma develops may be subject to legal frameworks in different countries or regions. In such cases, the accreditation entity refers to the relevant national bodies.

### 1.3.7 Trusted Service Provider (TSP).

A trusted service provider (TSP) is a natural person or legal entity who provides one or more trust services, whether a qualified or unqualified trusted service provider.

A qualified trusted service provider provides one or more qualified trusted services for which the supervisory body has granted the qualification.

The trusted services defined in eIDAS include:

- The creation, verification and validation of digital signatures. Certificates relating to these services are included.
- The creation, verification and validation of digital seals. Certificates relating to these services are included.
- The creation, verification and validation of digital timestamps. Certificates relating to these services are included.
- Certified digital delivery. Certificates relating to these services are included.
- The creation, verification and validation of certificates for website authentication.
- The preservation of digital signatures, seals or certificates related to these services.

### 1.3.8 Entity/Organisation.

The Entity is a public or private, individual or collective organisation, recognised under the law, with which the Subject maintains a certain relationship, as defined in the ORGANISATION field (O) in each certificate.

### 1.3.9 Applicant

Under this CPS, the Applicant is understood as the Signatory.

### 1.3.10 Certificate Holder/Key Holder

This CPS considers the certificate holder (the Subject) to be the person responsible for certificates issued to natural persons.

This CPS considers that the Signatory natural person submitting the application responsible for certificates issued to legal entities, even if the request is made via a third party, when it has knowledge of the existence of the certificate's existence.

For component certificates, this CPS considers the natural person, the Signatory submitting the application on their own behalf or via a third party to be the responsible party.

### 1.3.11 Hierarchies

This section describes the hierarchies and Certification Authorities (hereinafter CA or CAs) that Camerfirma manages. The use of hierarchies reduces the risks involved in issuing certificates and organising them in the different CAs.

> All the Certification Authorities (CAs) described can issue OCSP responder certificates. This certificate is used to sign and verify the OCSP service's responses regarding the status of the certificates issued by these CAs. The OID of certificates issued by each Certification Authority for issuing OCSP Responder certificates is 1.3.6.1.4.1.17326.10.9.8

Camerfirma manages two hierarchical structures:

- **Chambers of Commerce Root.**
- **Global Chambersign Root.**

As a general feature, the names of the CAs in the certificates issued to them are modified as they reach their expiry date, incorporating the year of issue. For example, the name of the CA may change to include the year of the certificate creation at the end of the name, although the characteristics will remain the same, unless otherwise stated in this CPS.

This CPS applies from **Chambers of Commerce Root 2016 and Global Chambersign Root 2016 hierarchies.**

#### 1.3.11.1 Issuing set test certificates and general test certificates.

Camerfirma issues certificates with a real hierarchy but with fictitious data in order to provide with them to regulatory entities, inspection procedures or new registration process, as well as for application developers in the process of integration or evaluation for acceptance. Camerfirma includes the following information in the certificates so that the User Party can clearly see that it is a test certificate without liability:

| | |
|---|---|
| **Name of the entity** | [TEST ONLY] ENTITY |
| **Entity Tax ID No.** | R05999990 |

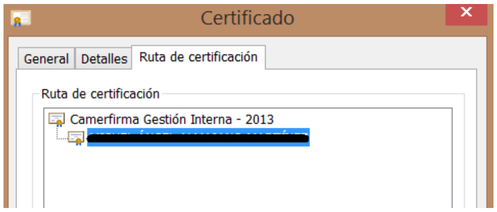
| | |
|---|---|
| **Entity address (street/number)** | ADDRESS |
| **Post code** | 5001 |
| **Contact telephone** | 902361207 |
| **Name** | JUAN |
| **First Surname** | CÁMARA |
| **Second Surname** | SPANISH |
| **National ID No.** | 00000000T |

When the accreditation and evaluation process requires the issuance of a test certificate with real data, the process is completed after signing a confidentiality agreement with the entity responsible for approval or evaluation tasks. The data is specific to each customer, but before the entity name [TEST ONLY] always appears in order to identify at first glance that it is a test certificate without liability.

### 1.3.11.2 Camerfirma Internal Management Hierarchy.

Camerfirma has developed a special certification authority to issue registration entity operator certificates. With this certificate, operators can perform the steps related to their own role on the Camerfirma STATUS® management platform.

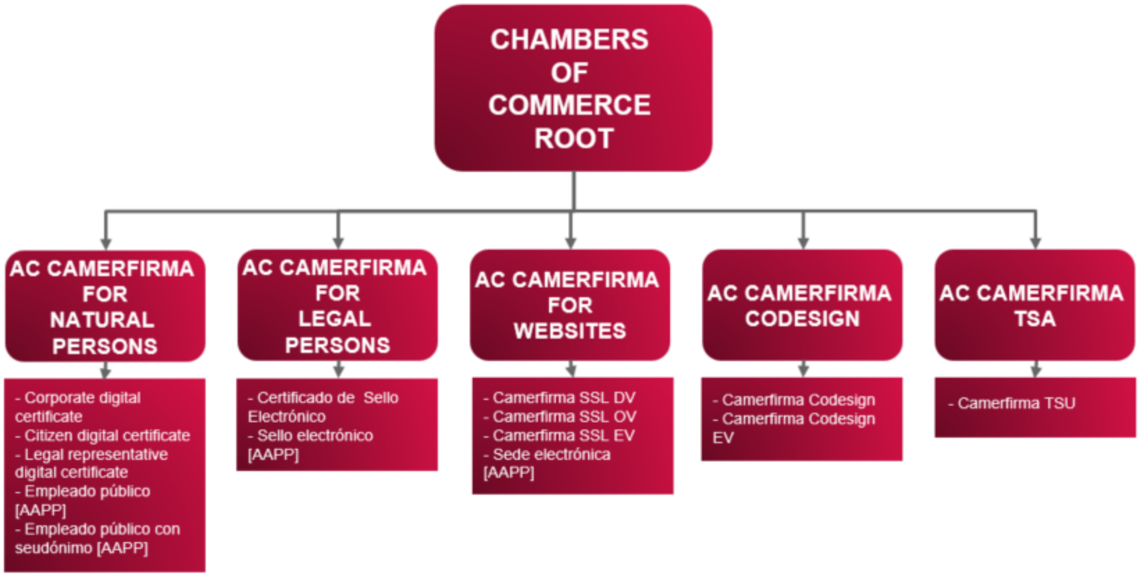
This hierarchy consists of a single CA that issues final entity certificates.



As a general design, the name of the CA certificates issued by Camerfirma includes the creation year of the associated cryptographic keys at the end, amending the corresponding year in each re-certification process.

### 1.3.11.3 CHAMBERS OF COMMERCE hierarchy.

**This hierarchy is applied since CHAMBERS OF COMMERCE 2016.**


CHAMBERS OF COMMERCE ROOT
AC CAMERFIRMA FOR NATURAL PERSONS
AC CAMERFIRMA FOR LEGAL PERSONS
AC CAMERFIRMA FOR WEBSITES
AC CAMERFIRMA CODESIGN
AC CAMERFIRMA TSA
- Corporate digital certificate
- Citizen digital certificate
- Legal representative digital certificate
- Empleado público [AAPP]
- Empleado público con seudónimo [AAPP]
- Certificado de Sello Electrónico
- Sello electrónico [AAPP]
- Camerfirma SSL DV
- Camerfirma SSL OV
- Camerfirma SSL EV
- Sede electrónica [AAPP]
- Camerfirma Codesign
- Camerfirma Codesign EV
- Camerfirma TSU

**CHAMBERS OF COMMERCE - Any Policy**

| **SHA256 Digital Fingerprint CHAMBERS OF COMMERCE - 2016** |
|---|
| 04:F1:BE:C3:69:51:BC:14:54:A9:04:CE:32:89:0C:5D:A3:CD:E1:35:6B:79:00:F6:E6:2D:FA:20:41:EB:AD:51 |
| **SHA-1 Digital Fingerprint CHAMBERS OF COMMERCE - 2016** |
| 2D:E1:6A:56:77:BA:CA:39:E1:D6:8C:30:DC:B1:4A:BE:22:A6:17:9B |
| **SHA256** Digital Fingerprint **CHAMBERS OF COMMERCE - 2018** |
| C4:B2:E2:2C:30:00:77:C2:8F:62:84:E0:F1:B0:CB:65:70:B1:6B:B2:64:96:9C:2E:A6:59:A5:45:CA:BA:A8:93 |
| **SHA-1** Digital Fingerprint **CHAMBERS OF COMMERCE - 2018** |
| C4:81:6D:04:0C:EB:CE:98:D8:CD:D0:4F:A5:E7:C2:A2:E2:92:DF:D2 |

This Hierarchy is designed to develop a trusted network, with the ultimate aim of issuing corporate, institutional and Public Administration digital identity certificates, within the European Union and in which the Registration Authorities (hereinafter RA or RAs) are managed by the Spanish Chambers of Commerce, Industry and Navigation or related public or private entities.

EXCEPTIONS: Component certificates (AC CAMERFIRMA CODESIGN, AC CAMERFIRMA TSA AND AC CAMERFIRMA FOR WEBSITES) have no territorial limitations and are not associated with specific registration entities.

Under this CPS, Intermediate Certification Authorities corresponding to a specific business, institution or public group can be issued, provided that the territory scope is the European Union. Thus the certificates issued under this intermediate certification authority acquire the recognition obtained by ROOT in commercial applications (read: Browsers such as Internet Explorer, Google Chrome, Mozilla Firefox, etc.).

On the other hand, the scheme of Intermediate Certification Authorities issuing digital certificates under this hierarchy is:

| **AC CAMERFIRMA FOR NATURAL PERSONS** | |
|---|---|
| **1.3.6.1.4.1.17326.10.16.1.1** | **CITIZEN DIGITAL CERTIFICATE** |
| 1.3.6.1.4.1.17326.10.16.1.1.1<br>0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd] | Qualified Citizen Certificate in QSCD |
| 1.3.6.1.4.1.17326.10.16.1.1.2<br>0.4.0.194112.1.0 [ETSI EN 319 411 2 - QCP-n] | Qualified Citizen Certificate |
| **1.3.6.1.4.1.17326.10.16.1.2** | **CORPORATE DIGITAL CERTIFICATE** |
| 1.3.6.1.4.1.17326.10.16.1.2.1<br>0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd] | Qualified Corporate Certificate in QSCD |
| 1.3.6.1.4.1.17326.10.16.1.2.2<br>0.4.0.194112.1.0 [ETSI EN 319 411 2 - QCP-n] | Qualified Corporate Certificate |
| **1.3.6.1.4.1.17326.10.16.1.3** | **LEGAL REPRESENTATIVE DIGITAL CERTIFICATE** |
| 1.3.6.1.4.1.17326.10.16.1.3.1.1<br>2.16.724.1.3.5.8 [Spanish regulation]<br>0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd] | Qualified Certificate for a Legal Entity Representative with general powers of representation in QSCD |
| 1.3.6.1.4.1.17326.10.16.1.3.1.2<br>2.16.724.1.3.5.8 [Spanish regulation]<br>0.4.0.194112.1.0 [ETSI EN 319 411 2 - QCP-n] | Qualified Certificate for a Legal Entity Representative with general powers of representation |
| 1.3.6.1.4.1.17326.10.16.1.3.1.1<br>2.16.724.1.3.5.9 [Spanish regulation]<br>0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd] | Qualified Certificate for a Representative of a Non-legal Entity with general powers of representation in QSCD |
| 1.3.6.1.4.1.17326.10.16.1.3.1.2<br>2.16.724.1.3.5.9 [Spanish regulation]<br>0.4.0.194112.1.0 [ETSI EN 319 411 2 - QCP-n] | Qualified Certificate for a Representative of a Non-legal Entity with general powers of representation |
| 1.3.6.1.4.1.17326.10.16.1.3.2.1<br>2.16.724.1.3.5.8 [Spanish regulation]<br>0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd] | Qualified Legal Entity Representative Certificate for procedures with the Public Administrations in QSCD |
| 1.3.6.1.4.1.17326.10.16.1.3.2.2<br>2.16.724.1.3.5.8 [Spanish regulation]<br>0.4.0.194112.1.0 [ETSI EN 319 411 2 - QCP-n] | Qualified Legal Entity Representative Certificate for procedures with the Public Administrations |
| 1.3.6.1.4.1.17326.10.16.1.3.2.1<br>2.16.724.1.3.5.9 [Spanish regulation]<br>0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd] | Qualified Certificate for a Representative of a Non-legal Entity for procedures with the Public Administrations in QSCD |
| 1.3.6.1.4.1.17326.10.16.1.3.2.2<br>2.16.724.1.3.5.9 [Spanish regulation]<br>0.4.0.194112.1.0 [ETSI EN 319 411 2 - QCP-n] | Qualified Certificate for a Representative of a Non-legal Entity for procedures with the Public Administrations |
| 1.3.6.1.4.1.17326.10.16.1.3.3.1<br>2.16.724.1.3.5.8 [Spanish regulation]<br>0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd] | Qualified Legal Entity Representative Certificate for Legal Representative in QSCD |
| 1.3.6.1.4.1.17326.10.16.1.3.3.2<br>2.16.724.1.3.5.8 [Spanish regulation]<br>0.4.0.194112.1.0 [ETSI EN 319 411 2 - QCP-n] | Qualified Legal Entity Representative Certificate for Legal Representatives |

| | |
|---|---|
| 1.3.6.1.4.1.17326.10.16.1.3.3.1<br>2.16.724.1.3.5.9 [Spanish regulation]<br>0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd] | Qualified Certificate for a Representative of a Non-legal Entity for Legal Representatives in QSCD |
| 1.3.6.1.4.1.17326.10.16.1.3.3.2<br>2.16.724.1.3.5.9 [Spanish regulation]<br>0.4.0.194112.1.0 [ETSI EN 319 411 2 - QCP-n] | Qualified Certificate for a Representative of a Non-legal Entity for Legal Representatives |
| **1.3.6.1.4.1.17326.10.16.1.5** | **PUBLIC EMPLOYEE [PUBLIC ADMINISTRATION]** |
| 1.3.6.1.4.1.17326.10.16.1.5.1.3.4.1<br>2.16.724.1.3.5.7.1 [PUBLIC ADMINISTRATION high-level public employee]<br>0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd] | Qualified Public Employee Signature Certificate in QSCD. High Level. |
| 1.3.6.1.4.1.17326.10.16.1.5.1.3.4.2<br>2.16.724.1.3.5.7.1 [Public Administration high-level public employee]<br>0.4.0.2042.1.2 [ETSI EN 319 411 1 - NCP+] | Public Employee Authentication Certificate in QSCD. High Level. |
| 1.3.6.1.4.1.17326.10.16.1.5.1.3.4.3<br>2.16.724.1.3.5.7.1 [Public Administration high-level public employee] | Public Employee Encrypted Certificate High Level. |
| 1.3.6.1.4.1.17326.10.16.1.5.1.3.4.4<br>2.16.724.1.3.5.7.2 [Public Administration mid-level public employee]<br>0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd] | Qualified Public Employee certificate in QSCD. Mid Level. |
| 1.3.6.1.4.1.17326.10.16.1.5.1.3.4.4<br>2.16.724.1.3.5.7.2 [Public Administration mid-level public employee]<br>0.4.0.194112.1.0 [ETSI EN 319 411 2 – QCP-n] | Public Employee Qualified Certificate. Mid Level. |
| 1.3.6.1.4.1.17326.10.16.1.5.1.3.4.1<br>2.16.724.1.3.5.7.1 [PUBLIC ADMINISTRATION high-level public employee]<br>0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd] | Qualified Public Employee Certificate with Signature Pseudonym in QSCD. High Level. |
| 1.3.6.1.4.1.17326.10.16.1.5.1.3.4.2<br>2.16.724.1.3.5.7.1 [Public Administration high-level public employee]<br>0.4.0.2042.1.2 [ETSI EN 319 411 1 - NCP+] | Certificate for Public Employee with Signature Authentication in QSCD. High Level. |
| 1.3.6.1.4.1.17326.10.16.1.5.1.3.4.3<br>2.16.724.1.3.5.7.1 [Public Administration high-level public employee] | Public Employee Certificate with Encrypted Pseudonym. High Level. |
| 1.3.6.1.4.1.17326.10.16.1.5.1.3.4.4<br>2.16.724.1.3.5.7.2 [Public Administration mid-level public employee]<br>0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd] | Qualified Public Employee Certificate with Pseudonym in QSCD |
| 1.3.6.1.4.1.17326.10.16.1.5.1.3.4.4<br>2.16.724.1.3.5.7.2 [Public Administration mid-level public employee]<br>0.4.0.194112.1.0 [ETSI EN 319 411 2 - QCP-n] | Qualified Public Employee Certificate with Pseudonym. Mid Level. |
| **AC CAMERFIRMA FOR LEGAL PERSONS** | |
| 1.3.6.1.4.1.17326.10.16.2.1 | **DIGITAL SEAL QUALIFIED DIGITAL CERTIFICATE** |
| 1.3.6.1.4.1.17326.10.16.2.1.1<br>0.4.0.194112.1.3 [ETSI EN 319 411 2 - QCP-l-qscd] | Qualified Digital Seal Certificate in QSCD |
| 1.3.6.1.4.1.17326.10.16.2.1.2<br>0.4.0.194112.1.1 [ETSI EN 319 411 2 - QCP-l] | Qualified Digital Seal Certificate |
| 1.3.6.1.4.1.17326.10.16.2.3 | **DIGITAL SEAL DIGITAL CERTIFICATE** |
| 1.3.6.1.4.1.17326.10.16.2.3.2<br>0.4.0.2042.1.3 [ETSI EN 319 411 1 - LCP] | Digital Seal Certificate |
| 1.3.6.1.4.1.17326.10.16.2.2 | **DIGITAL SEAL (PUBLIC ADMINISTRATION)** |
| 1.3.6.1.4.1.17326.10.16.2.2.1.3.3.1<br>0.4.0.194112.1.3 [ETSI EN 319 411 2 - QCP-l-qscd]<br>2.16.724.1.3.5.6.1 [PUBLIC ADMINISTRATION - high level seal] | Public Administrations Digital Seal Certificate in QSCD. High Level. |

| | |
|---|---|
| 1.3.6.1.4.1.17326.10.16.2.2.1.4.3.1<br>0.4.0.194112.1.3 [ETSI EN 319 411 2 - QCP-l-qscd]<br>OID 2.16.724.1.3.5.6.2 [PUBLIC ADMINISTRATION - mid level seal] | Public Administrations Digital Seal Certificate in QSCD. Mid Level. |
| 1.3.6.1.4.1.17326.10.16.2.2.1.4.3.1<br>0.4.0.194112.1.1 [ETSI EN 319 411 2 - QCP-l]<br>OID 2.16.724.1.3.5.6.2 [PUBLIC ADMINISTRATION - mid level seal] | Public Administrations Digital Seal Certificate. Mid Level. |
| **AC CAMERFIRMA FOR WEBSITES** | |
| 1.3.6.1.4.1.17326.10.16.3.2 | **CAMERFIRMA SSL OV** |
| 1.3.6.1.4.1.17326.10.16.3.2.2<br>0.4.0.2042.1.7 [ETSI TS 102 042 - OVCP]<br>2.23.140.1.2.2 [CA/B FORUM - SSL OV] | OV Website Certificate |
| 1.3.6.1.4.1.17326.10.16.3.5 | **CAMERFIRMA SSL EV** |
| 1.3.6.1.4.1.17326.10.16.3.5.1<br>0.4.0.194112.1.4 [ETSI EN 319 411 2 - QCP-w]<br>2.23.140.1.1 [CA/B FORUM - SSL EV] | Qualified EV Website Certificate |
| 1.3.6.1.4.1.17326.10.16.3.6 | **GOVERNMENT ELECTRONIC OFFICE (Public Administration)** |
| 1.3.6.1.4.1.17326.10.16.3.6.1.3.2.1<br>0.4.0.194112.1.4 [ETSI EN 319 411 2 - QCP-w]<br>2.16.724.1.3.5.5.1 [Public Administrations - high level office]<br>2.23.140.1.1 [CA/B FORUM - SSL EV] | Qualified Digital Office Certificate - High Level - EV |
| 1.3.6.1.4.1.17326.10.16.3.6.1.3.2.2<br>0.4.0.194112.1.4 [ETSI EN 319 411 2 - QCP-w]<br>2.16.724.1.3.5.5.2 [Public Administrations - Mid Level office]<br>2.23.140.1.1 [CA/B FORUM - SSL EV] | Qualified Digital Office Certificate - Mid-level – EV |
| 1.3.6.1.4.1.17326.10.16.3.6.1.3.2.1<br>0.4.0.194112.1.4 [ETSI EN 319 411 2 - QCP-w]<br>2.16.724.1.3.5.5.1 [Public Administrations - high level office]<br>2.23.140.1.2.2 [CA/B FORUM - SSL OV] | Qualified Digital Office Certificate - High Level - OV |
| 1.3.6.1.4.1.17326.10.16.3.6.1.3.2.2<br>0.4.0.194112.1.4 [ETSI EN 319 411 2 - QCP-w]<br>2.16.724.1.3.5.5.2 [Public Administrations - Mid Level office]<br>2.23.140.1.2.2 [CA/B FORUM - SSL OV] | Qualified Digital Office Certificate - Mid-level - OV |
| **AC CAMERFIRMA CODESIGN** | |
| 1.3.6.1.4.1.17326.10.16.4.1 | **CAMERFIRMA CODESIGN** |
| 1.3.6.1.4.1.17326.10.16.4.1.1<br>0.4.0.194112.1.3 [ETSI EN 319 411 2 - QCP-l-qscd] | Qualified CodeSign Certificate in QSCD |
| 1.3.6.1.4.1.17326.10.16.4.1.2<br>0.4.0.194112.1.1 [ETSI EN 319 411 2 - QCP-l] | Qualified CodeSign Certificate |
| 1.3.6.1.4.1.17326.10.16.4.2 | **CAMERFIRMA EV CODESIGN** |
| 1.3.6.1.4.1.17326.10.16.4.2.1<br>0.4.0.194112.1.3 [ETSI EN 319 411 2 - QCP-l-qscd]<br>2.23.140.1.3 [CA/B FORUM - CODESIGN] | Qualified EV CodeSign Certificate in QSCD |
| 1.3.6.1.4.1.17326.10.16.4.2.2<br>0.4.0.194112.1.1 [ETSI EN 319 411 2 - QCP-l]<br>2.23.140.1.3 [CA/B FORUM - CODESIGN] | Qualified EV CodeSign Certificate |
| **AC CAMERFIRMA TSA** | |
| 1.3.6.1.4.1.17326.10.16.5.1 | **CAMERFIRMA TSU** |
| 1.3.6.1.4.1.17326.10.16.5.1.1<br>0.4.0.194112.1.3 [ETSI EN 319 411 2 - QCP-l-qscd] | TSU certificate on QSCD |
| 1.3.6.1.4.1.17326.10.16.5.1.2 | TSU certificate |

### *1.3.11.3.1 AC CAMERFIRMA FOR WEBSITES. (Website certificates)*

The intermediate CA issues digital certificates to HTML page server applications on the internet using the TLS protocol. This protocol is required to identify and establish secure channels between the user's or User Party's browser and the Subject/Signatory's HTML web server.

**Under this CPS, certificates can be issued to entities or organisations residing outside of the European Union. The procedure for issuing the certificate is covered in the relevant section of this CPS.**

Certificates are issued in different ways:

#### 1.3.11.3.1.1 **OV Website Certificates (*Organisation Validation*) – OVCP.**

Issuing this type of certificate complies with the requirements established by the document *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates* drafted by the CA/BROWSER FORUM http://www.cabforum.org. The registration processes include validating an organisation associated with the domain control.

#### 1.3.11.3.1.2 **Qualified EV Website Certificates (*Extended Validation*) –**

EVCP. The issuance of digital certificates for EV Secure Servers meets the requirements set forth in the document Guidelines for Issuance and Management of extended validation certificates, written by the CA/BROWSER FORUM http://www.cabforum.org. This regulation promotes the issuing of secure server certificates with extra guarantees in the certificate holders' identification process. ***An EV Website certificate gives browsers who connect to this service an extra level of guarantee, which can be seen from the green background in the browser address bar.***

#### 1.3.11.3.1.3 **Qualified OV and EV Digital Office Certificates - QCP-w.**

Established in Law 39/2015, 1 October, Public Administration Common Administrative Procedures.

### *1.3.11.3.2 AC CAMERFIRMA FOR LEGAL PERSONS. (Certificates for legal entities).*

#### 1.3.11.3.2.1 **Qualified Digital Seal Certificate – QCP-l, QCP-l-qscd.**

This certificate is issued to a legal entity whose applicant must have representation or authorisation from the entity included in the certificate. This certificate can be associated with a key activated by a machine or application. Common transactions can be carried out automatically and without requiring intervention. The keys associated with the use of a digital seal certificate provide integrity and authenticity to the documents and transactions to which they apply. It can also be used as a client machine identification element in secure TLS communication protocols.

1.3.11.3.2.2 **Digital Seal Certificate – LCP.**

This certificate is issued to a legal entity whose applicant must have representation or authorisation from the entity included in the certificate. This certificate can be associated with a key activated by a machine or application. Common transactions can be carried out automatically and without requiring intervention. The keys associated with the use of a digital seal certificate provide integrity and authenticity to the documents and transactions to which they apply. It can also be used as a client machine identification element in secure TLS communication protocols.

1.3.11.3.2.3 **Public Administrations Digital Seal Certificate. QCP-l, QCP-l-qscd**

Established in Law 39/2015, 1 October, Public Administration Common Administrative Procedures.

### *1.3.11.3.3 AC CAMERFIRMA CODESIGN. (CodeSign certificates).*

Intermediate CA called "AC CAMERFIRMA CODESIGN" that issues CodeSign certificates. As the name suggests, CodeSign certificates enable developers to apply a digital signature to the code they have developed: ActiveX, Java applets, Microsoft Office macros, etc., thus guaranteeing the integrity and authenticity of this code.

**Under this CPS, certificates can be issued to entities or organisations residing outside of Spanish territory. The procedure for issuing the certificate is covered in the relevant section of this CPS.**

Certificates are issued in different ways:

1.3.11.3.3.1 **Qualified CodeSign Certificates – QCP-l, QCP-l-qscd.**

Issuing this type of certificate complies with the requirements established by the document *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates* drafted by the CA/BROWSER FORUM http://www.cabforum.org. The registration processes include validating an organisation associated with the domain control.

1.3.11.3.3.2 **Qualified EV CodeSign Certificates (*Extended Validation*) – QCP-l, QCP-l-qscd.**

The issuance of EV CodeSign digital certificates is subject to the requirements set forth in the document *Guidelines For The Issuance And Management Of*

*Extended Validation Code Signing Certificates* written by the CA/BROWSER FORUMhttp://www.cabforum.org. This regulation promotes the issuing of CodeSign certificates with extra guarantees in the certificate holders' identification process.

### *1.3.11.3.4 AC CAMERFIRMA TSA. (Timestamp certificates)*

This authority issues certificates for **issuing timestamps**. A Timestamp is a data packet with a standardised structure that associates the summary code or *hash* code of a document or digital transaction with a specific date and time.

The time-stamping authority issues certificates to intermediate entities called "Timestamping Units" **TSU**. These timestamp units ultimately issue the timestamps on receiving a standard request in accordance with the **RFC 3161** specifications. Each of these **TSUs** can be associated either with the service's specific technical features or exclusive client use.

**TSU certificates have a six-year duration and use of a private key for one year, so the time certificates issued by these TSUs time have a minimum duration of five years.**

**Under this CPS, TSU certificates can be issued to companies and entities residing outside of Spanish territory. The procedure for issuing the certificate is covered in the relevant section of this CPS.**

AC Camerfirma issues TSU certificates on **equipment accredited** by AC Camerfirma. The accredited equipment may be located on the premises of the Signatory through the signature of an affidavit and compliance with the requirements associated with issuing a TSU certificate.

AC Camerfirma also issues TSU certificates for storage on **third party platforms** as long as these platforms:

- Are synchronised with the timestamps established by Camerfirma.
- Allow Camerfirma or an authorised third party to audit the systems.
- Allow AC Camerfirma signing applications access to their service in order to establish the appropriate controls regarding the correction of the timestamp.
- Sign a service agreement.
- Provide access to AC Camerfirma to collect information about the seals issued or submit a periodic report on the number of seals issued.
- Submit a key creation record in a safe environment as indicated by Camerfirma's TSA certification policies (HSM FIPS 140-1 Level 3 certificate) signed by a competent organisation. This record is first reviewed and signed by AC Camerfirma technical personnel before validation is given.

The TSU certificate policies are:

1.3.11.3.4.1 **Qualified TSU certificate in QSCD**

The keys are generated and stored in a HSM FIPFS 140-1 Level 2 certificate.

1.3.11.3.4.2 **TSU certificate**

The keys are generated and stored in software media.

Access to the service is authenticated by username/password or digital certificate. IP authentication implementations are also permitted.

Further information at http://www.camerfirma.com/servicios/sellado-de-tiempo

### *1.3.11.3.5 AC CAMERFIRMA FOR NATURAL PERSONS. (Certificates for natural persons)*

Camerfirma is a multi-policy Certification Authority that issues qualified and non-qualified certificates for natural persons within the European Union whose functionalities are described below.

The final certificates are intended for:

1.3.11.3.5.1 **Natural persons with a business relationship with an Entity.**

1.3.11.3.5.1.1 Qualified Corporate Certificate – QCP-n, QCP-n-qscd.

These determine the type of contractual relationship (labour, mercantile, institution, etc.) between a natural person (Certificate Holder/Subject/Signatory) and an Entity (certificate's organisation field).

1.3.11.3.5.1.2 Qualified Legal Representative Certificate:

1.3.11.3.5.1.2.1 *Qualified Certificate for a Representative of a Legal Entity with general powers of representation. – QCP-n, QCP-n-qscd.*

This determines the powers of legal representation or general power of attorney between the natural person (Certificate Holder/Subject/Signatory) and an Entity with legal status (also described in the Certificate's organisation field).

1.3.11.3.5.1.2.2 *Qualified Certificate for a Representative of a Non-legal Entity with general powers of representation – QCP-n, QCP-n-qscd.*

This determines the powers of legal representation or general power of attorney between the natural person (Certificate Holder/Subject/Signatory) and an Entity without legal status (also described in the Certificate's organisation field).

1.3.11.3.5.1.2.3 *Qualified Legal Entity Representative Certificate for procedures with the Public Administrations. – QCP-n, QCP-n-qscd.*

Its purpose is to identify an individual and add the attribute (information) that such person may represent in an entity with legal status in the field of Public Administration.

1.3.11.3.5.1.2.4 *Qualified Certificate for a Representative of a Non-legal Entity for procedures with the Public Administrations. – QCP-n, QCP-n-qscd.*

Its purpose is to identify an individual and add the attribute (information) that such person may represent in an entity with no legal status in the field of Public Administration.

1.3.11.3.5.1.2.5 *Qualified Legal Entity Representative Certificate for Legal Representatives. – QCP-n, QCP-n-qscd.*

This determines the powers of specific representation or special power of attorney between the natural person (certificate holder/Subject/Signatory) and an Entity with legal status (also described in the Certificate's organisation field).

1.3.11.3.5.1.2.6 *Qualified Non-Legal Entity Representative Certificate for Legal Representatives. – QCP-n, QCP-n-qscd.*

This determines the powers of specific representation or special power of attorney between the natural person (certificate holder/Subject/Signatory) and an Entity without legal status (also described in the Certificate's organisation field).

1.3.11.3.5.1.3 Public Employee Certificates. – QCP-n, QCP-n-qscd, NCP+.

Established in Law 39/2015, 1 October, Public Administration Common Administrative Procedures.

The legal framework provides various solutions to many problems that currently exist in relation to digital identification and signing for Public Administrations, including with citizens and companies, and with public sector employees.

The General State Administration (GSA) has defined a certification model that includes public certification service providers but also the possibility of bodies dependent on the GSA being able to contract private certification service providers.

This model is mixed, due to being a regulated free market model, in which private certification service providers could be contracted by any body dependent on the Public Administration to provide certification services.

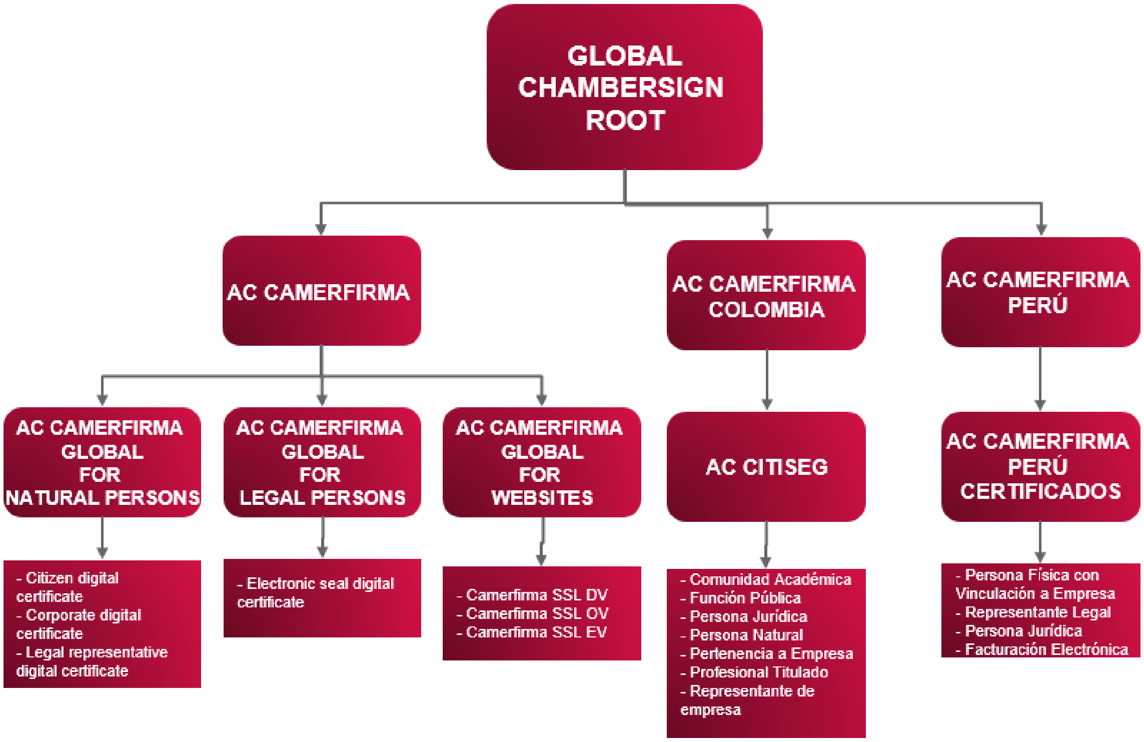
1.3.11.3.5.2 **Natural persons WITH NO business relationship with an Entity.**

1.3.11.3.5.2.1 Qualified Citizen Certificate. – QCP-n, QCP-n-qscd.

Determines the identity of the natural person signatory to act on his/her own behalf.

### 1.3.11.4 GLOBAL CHAMBERSIGN ROOT hierarchy.

**This hierarchy applies from GLOBAL CHAMBERSIGN ROOT - 2016.**


GLOBAL CHAMBERSIGN ROOT
AC CAMERFIRMA
AC CAMERFIRMA COLOMBIA
AC CAMERFIRMA PERÚ
AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS
AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS
AC CAMERFIRMA GLOBAL FOR WEBSITES
AC CITISEG
AC CAMERFIRMA PERÚ CERTIFICADOS
- Citizen digital certificate
- Corporate digital certificate
- Legal representative digital certificate
- Electronic seal digital certificate
- Camerfirma SSL DV
- Camerfirma SSL OV
- Camerfirma SSL EV
- Comunidad Académica
- Función Pública
- Persona Jurídica
- Persona Natural
- Pertenencia a Empresa
- Profesional Titulado
- Representante de empresa
- Persona Física con Vinculación a Empresa
- Representante Legal
- Persona Jurídica
- Facturación Electrónica

### GLOBAL CHAMBERSIGN ROOT - AnyPolicy.

| **SHA-256 Digital Fingerprint** |
|---|
| C1:D8:0C:E4:74:A5:11:28:B7:7E:79:4A:98:AA:2D:62:A0:22:5D:A3:F4:19:E5:C7:ED:73:DF:BF:66:0E:71:09 |
| **SHA-1 Digital Fingerprint** |
| 11:39:A4:9E:84:84:AA:F2:D9:0D:98:5E:C4:74:1A:65:DD:5D:94:E2 |

This hierarchy is created for issuing certificates for specific projects with a specific Entity or Entities. It is therefore an open hierarchy in which certificates and their management are adapted to specific project needs. In this sense, unlike the “Chambers of Commerce Root” mentioned above, the Registration Authorities are not necessarily included within the scope of the Spanish Chambers of Commerce, or within a specific regional scope, business scope or a business relationship. This hierarchy can therefore issue certificates anywhere there is a recognised RA that meets Camerfirma’s requirements, always subject to current law and applicable to international trading relations.

The ChamberSign Global Root Hierarchy organises the issuance of digital certificates in different territories by establishing certification authorities created specifically for issuing certificates in a particular country, thus allowing better adaptation to the legal framework and corresponding regulations.

Within the framework of this hierarchy, there are different intermediate certification authorities that correspond to global, national, sector and corporate frameworks.

| | |
|---|---|
| **GLOBAL CHAMBERSIGN ROOT - 2016** | |
| **AC CAMERFIRMA**<br>**AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS** | |
| **1.3.6.1.4.1.17326.20.16.1.1.1** | **CITIZEN DIGITAL CERTIFICATE** |
| 1.3.6.1.4.1.17326.20.16.1.1.1.1 | Citizen Certificate in QSCD |
| 1.3.6.1.4.1.17326.20.16.1.1.1.2 | Citizen certificate |
| **1.3.6.1.4.1.17326.20.16.1.1.2** | **CORPORATE DIGITAL CERTIFICATE** |
| 1.3.6.1.4.1.17326.20.16.1.1.2.1 | Corporate certificate in QSCD |
| 1.3.6.1.4.1.17326.20.16.1.1.2.2 | Corporate certificate |
| **1.3.6.1.4.1.17326.20.16.1.1.3** | **LEGAL REPRESENTATIVE DIGITAL CERTIFICATE** |
| 1.3.6.1.4.1.17326.20.16.1.1.3.1.1 | Legal Entity Representative Certificate in QSCD |
| 1.3.6.1.4.1.17326.20.16.1.1.3.1.2 | Legal Entity Representative Certificate |
| 1.3.6.1.4.1.17326.20.16.1.1.3.2.1 | Non-Corporate Entity Representative Certificate in QSCD |
| 1.3.6.1.4.1.17326.20.16.1.1.3.2.2 | Non-Corporate Entity Representative Certificate |
| **AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS** | |
| **1.3.6.1.4.1.17326.20.16.1.2.1** | **DIGITAL SEAL DIGITAL CERTIFICATE** |
| 1.3.6.1.4.1.17326.20.16.1.2.1.1.1 | Digital Seal Certificate in QSCD |
| 1.3.6.1.4.1.17326.20.16.1.2.1.1.2 | Digital Seal Certificate |
| **AC CAMERFIRMA GLOBAL FOR WEBSITES** | |
| **1.3.6.1.4.1.17326.10.8.12** | **CAMERFIRMA SSL EV** |
| 1.3.6.1.4.1.17326.10.8.12.1.2 | EV Website Certificate |
| **AC CAMERFIRMA GLOBAL TSA** | |
| **1.3.6.1.4.1.17326.20.16.1.3.1** | **CAMERFIRMA GLOBAL TSU** |
| 1.3.6.1.4.1.17326.20.16.1.3.1.1 | Certificado de GLOBAL TSU QSCD |
| 1.3.6.1.4.1.17326.20.16.1.3.1.2 | Certificado de GLOBAL TSU |
| **AC CAMERFIRMA COLOMBIA**<br>**AC CITISEG** | |
| **1.3.6.1.4.1.17326.20.1.1** | **ACADEMIC COMMUNITY** |
| 1.3.6.1.4.1.17326.20.1.1.2 | Academic Community Certificate |
| **1.3.6.1.4.1.17326.20.1.2** | **PUBLIC OFFICIAL** |
| 1.3.6.1.4.1.17326.20.1.2.2 | Public Official Certificate |
| **1.3.6.1.4.1.17326.20.1.3** | **LEGAL ENTITY** |
| 1.3.6.1.4.1.17326.20.1.3.2 | Legal Entity Certificate |
| **1.3.6.1.4.1.17326.20.1.4** | **NATURAL PERSON** |
| 1.3.6.1.4.1.17326.20.1.4.2 | Natural person certificate |
| **1.3.6.1.4.1.17326.20.1.5** | **BELONGING TO A COMPANY** |
| 1.3.6.1.4.1.17326.20.1.5.2 | Contractual Relationship Certificate |
| **1.3.6.1.4.1.17326.20.1.6** | **QUALIFIED PROFESSIONAL** |
| 1.3.6.1.4.1.17326.20.1.6.2 | Qualified Professional Certificate |

| | |
|---|---|
| **1.3.6.1.4.1.17326.20.1.7** | **COMPANY REPRESENTATIVE** |
| 1.3.6.1.4.1.17326.20.1.7.2 | Company Representative Certificate |
| **AC CAMERFIRMA PERU**<br>**AC CAMERFIRMA PERU CERTIFICATES** | |
| **1.3.6.1.4.1.17326.30.16.0** | **PHYSICAL PERSON WITH COMPANY LINK** |
| 1.3.6.1.4.1.17326.30.16.0.1 | Certificate for a natural person linked to a company |
| **1.3.6.1.4.1.17326.30.16.10** | **LEGAL REPRESENTATIVE** |
| 1.3.6.1.4.1.17326.30.16.10.1 | Legal Representative Certificate |
| **1.3.6.1.4.1.17326.30.16.20** | **LEGAL ENTITY** |
| 1.3.6.1.4.1.17326.30.16.20.1 | Legal Entity Certificate |
| **1.3.6.1.4.1.17326.30.16.30** | **DIGITAL INVOICING** |
| 1.3.6.1.4.1.17326.30.16.30.1 | Digital Invoicing Certificate |
| **1.3.6.1.4.1.17326.30.16.40** | **PHYSICAL PERSON** |
| 1.3.6.1.4.1.17326.30.16.40.1 | Physical Person Certificate |
| **1.3.6.1.4.1.17326.30.16.50** | **ENTITY’S ELECTRONIC SEAL** |
| 1.3.6.1.4.1.17326.30.16.50.1 | Entity’s Electronic Seal Certificate |

### *1.3.11.4.1 AC CAMERFIRMA.*

The purpose of this intermediate CA is to issue Subordinate CA certificates with no restrictions in the specific geographical, sectoral or registration authority areas.

#### 1.3.11.4.1.1 **AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS (Certificates for natural persons)**

This Certification Authority issues certificates for natural persons with no restrictions on specific geographical, sectoral or registration authority areas.

##### 1.3.11.4.1.1.1 Natural persons with a business relationship with an Entity.

1.3.11.4.1.1.1.1 *Corporate certificate.*

These determine the type of contractual relationship (labour, mercantile, institution, etc.) between a natural person (Certificate Holder/Subject/Signatory) and an Entity (certificate's organisation field).

1.3.11.4.1.1.1.2 *Legal Entity Representative Certificate.*

This determines the powers of legal representation or general power of attorney between the natural person (Certificate Holder/Subject/Signatory) and an Entity with legal status (also described in the Certificate's organisation field).

1.3.11.4.1.1.1.3 *Non-Corporate Entity Representative Certificate.*

This determines the powers of legal representation or general power of attorney between the natural person (Certificate

Holder/Subject/Signatory) and an Entity without legal status (also described in the Certificate's organisation field).

1.3.11.4.1.1.2 Natural persons WITH NO business relationship with an Entity.

1.3.11.4.1.1.2.1 *Citizen Certificate.*

Determines the identity of the natural person signatory to act on his/her own behalf.

1.3.11.4.1.2 **AC CAMERFIRMA GLOBAL FOR LEGAL ENTITIES. (Certificates for legal entities)**

1.3.11.4.1.2.1 Digital Seal Certificate.

This certificate is issued to a legal entity whose applicant must have representation or authorisation from the entity included in the certificate. This certificate can be associated with a key activated by a machine or application. Common transactions can be carried out automatically and without requiring intervention. The keys associated with the use of a digital seal certificate provide integrity and authenticity to the documents and transactions to which they apply. It can also be used as a client machine identification element in secure TLS communication protocols.

1.3.11.4.1.3 **AC CAMERFIRMA GLOBAL FOR WEBSITES. (Website certificates). EVCP.**

The intermediate CA issues digital certificates to HTML page server applications on the internet using the TLS protocol. This protocol is required to identify and establish secure channels between the user's or User Party's browser and the Subject/Signatory's HTML web server.

This CA issues certificates in the same manner and scope as its equivalent in the Chambers of Commerce Root hierarchy.

1.3.11.4.1.4 **AC CAMERFIRMA GLOBAL TSA. (TSU certificates).**

This authority issues certificates for **issuing timestamps**. A Timestamp is a data packet with a standardised structure that associates the summary code or *hash* code of a document or digital transaction with a specific date and time.

**TSU certificates have a six-year duration and use of a private key for one year, so the time certificates issued by these TSUs time have a minimum duration of five years.**

**Under this CPS, TSU certificates can be issued to companies and entities residing outside of Spanish territory. The procedure for issuing the certificate is covered in the relevant section of this CPS.**

AC Camerfirma issues TSU certificates on **equipment accredited** by AC Camerfirma. The accredited equipment may be located on the premises of the Signatory through the signature of an affidavit and compliance with the requirements associated with issuing a TSU certificate.

AC Camerfirma also issues TSU certificates for storage on **third party platforms** as long as these platforms:

- Are synchronised with the timestamps established by Camerfirma.
- Allow Camerfirma or an authorised third party to audit the systems.
- Allow AC Camerfirma signing applications access to their service in order to establish the appropriate controls regarding the correction of the timestamp.
- Sign a service agreement.
- Provide access to AC Camerfirma to collect information about the seals issued or submit a periodic report on the number of seals issued.
- Submit a key creation record in a safe environment as indicated by Camerfirma's TSA certification policies (HSM FIPS 140-1 Level 3 certificate) signed by a competent organisation. This record is first reviewed and signed by AC Camerfirma technical personnel before validation is given.

The TSU certificate policies are:

###### 1.3.11.4.1.4.1 Global TSU certificate in QSCD

The keys are generated and stored in a HSM FIPFS 140-1 Level 2 certificated.

###### 1.3.11.4.1.4.2 Global TSU certificate

The keys are generated and stored in software media.

Access to the service is authenticated by username/password or digital certificate. IP authentication implementations are also permitted.

Further information at http://www.camerfirma.com/servicios/sellado-de-tiempo

###### 1.3.11.4.1.5 **AC CAMERFIRMA COLOMBIA.**

The purpose of this intermediate CA is to issue Subordinate CA certificates within the geographical scope of the Republic of Colombia.

1.3.11.4.1.6 **AC CITISEG (Certificates for natural and legal entities)**

1.3.11.4.1.6.1 Academic Community Certificate (Certificates for natural persons)

These determine the type of contractual relationship (labour, mercantile, member of professional body, etc.) between a natural person (Certificate Holder/Subject/Signatory) and an Academic Entity (certificate's organisation field).

1.3.11.4.1.6.2 Public Official Certificate (Certificates for natural persons)

They determine the employment relationship between a natural person (certificate holder/Subject/Signatory) and an Entity belonging to the Public Administration of the Republic of Colombia (certificate organisation field).

1.3.11.4.1.6.3 Legal Entity Certificate (Certificates for legal entities)

This certificate is issued to a legal entity whose applicant must have representation or authorisation from the entity included in the certificate. This certificate can be associated with a key activated by a machine or application. Common transactions can be carried out automatically and without requiring intervention. The keys associated with the use of a digital seal certificate provide integrity and authenticity to the documents and transactions to which they apply. It can also be used as a client machine identification element in secure TLS communication protocols.

1.3.11.4.1.6.4 Natural Person Certificate (Certificates for natural persons)

Determines the identity of the natural person signatory to act on his/her own behalf.

1.3.11.4.1.6.5 Contractual Relationship Certificate **(Certificates for natural persons)**

These determine the type of employment or commercial contractual relationship between a natural person (Certificate Holder/Subject/Signatory) and an Entity (certificate's organisation field).

1.3.11.4.1.6.6 Qualified Professional Certificate (Certificates for natural persons)

These determine the type of professional relationship between a natural person (Certificate Holder/Subject/Signatory) and an Institutional Entity (certificate's organisation field).

1.3.11.4.1.6.7 Company Representative Certificate (Certificates for natural persons)

This determines the powers of legal representation or general power of attorney between the natural person (Certificate Holder/Subject/Signatory) and an Entity with legal status (also described in the Certificate's organisation field).

1.3.11.4.1.7 **AC CAMERFIRMA PERU.**

The purpose of this intermediate CA will be to issue Subordinate CA certificates within the geographic scope of the Republic of Peru.

1.3.11.4.1.7.1 AC CAMERFIRMA PERU CERTIFICATES (Certificates for natural and legal entities)

1.3.11.4.1.7.1.1 *Certificate of Natural persons with a contractual relationship with a company (Certificates for natural persons)*

These determine the type of employment or commercial contractual relationship between a natural person (Certificate Holder/Subject/Signatory) and an Entity (certificate's organisation field).

1.3.11.4.1.7.1.2 *Legal Representative Certificate (Certificates for natural persons)*

This determines the powers of legal representation or general power of attorney between the natural person (Certificate Holder/Subject/Signatory) and an Entity with legal status (also described in the Certificate's organisation field).

1.3.11.4.1.7.1.3 *Legal Entity Certificate (Certificates for legal entities)*

This certificate is issued to a legal entity whose applicant must have representation or authorisation from the entity included in the certificate. This certificate can be associated with a key activated by a machine or application. Common transactions can be carried out automatically and without requiring intervention. The keys associated with the use of a digital seal certificate provide integrity and authenticity to the documents and transactions to which they apply. It can also be used as a client machine identification element in secure TLS communication protocols.

1.3.11.4.1.7.1.4 *Electronic Invoice Certificate (Certificates for natural persons)*

This certificate is exclusively made for generating digital invoices and is issued to a legal entity whose applicant must have representation or authorisation from the entity included in the certificate. The action of the keys associated with the use of a contractual relationship certificate provides integrity and authenticity to the invoices to which they are applied

1.3.11.4.1.7.1.5 *Physical Person Certificate (Certificates for individuals)*

Determine the identity of the physical person signing to act on their own behalf.

1.3.11.4.1.7.1.6 *Electronic Invoice Certificate (Certificates for natural persons)*

This certificate is issued to a legal entity whose applicant must have representation or authorization from the entity included in the certificate. This certificate can be associated with a key activated by a machine or application. The operations carried out are usually carried out automatically and unassisted. The action of the keys is associated with the use of an electronic seal certificate that provides integrity and authenticity to the documents and transactions to which it applies. It is also allowed to be used as a machine customer identification element in secure TLS communication protocols.

## *1.4 Scope of Application and Usage*

This CPS fulfils the Certification Policies described in section 1.3.11 of this CPS.

### 1.4.1 Appropriate Certificate Uses

Camerfirma certificates can be used in accordance with the terms and conditions set out in the Certification Policies.

In general terms, certificates are issued for the following uses:

- **Authentication** based on X.509v3 certificates.
- **Digital signature**, advanced or qualified, based on X.509v3 certificates.
- **Asymmetric or mixed encryption**, based on X.509v3 certificates.

### 1.4.2 Prohibited and Unauthorised Certificate Uses

The certificates can only be used for the purposes for which they were issued and are subject to the limits defined in the certification policies.

Certificates are not designed, may not be used and their use or resale is not authorised as control equipment for dangerous situations or for uses requiring fail-safe actions, such as the operation of nuclear facilities, navigation systems or aerial communication or weapon control systems, where an error could directly result in death, personal injury, or severe environmental damage.

The use of digital certificates in transactions that contravene the Certification Policies applicable to each of the Certificates, the CPS or the Contracts that the CAs sign with the RAs or with the Signatory (Subjects) and/or Signatories is considered illegal, and the CA is exempt from any liability due to the Signatory or third party's misuse of the certificates in accordance with current law.

Camerfirma does not have access to the data for which a certificate is used. Therefore, due to lack of access to message contents, Camerfirma cannot issue any appraisal regarding these contents and the Signatory is consequently responsible for the data for which the certificate is used. The Signatory is also responsible for the consequences of any use of this data in breach of the limitations and terms and conditions established in the Certification Policies applicable to each Certificate, the CPS and the contracts the CAs sign with the Signatory (Subject), as well as any misuse thereof in accordance with this paragraph or which could be interpreted as such by virtue of current law.

In the certificate information on the limitation of use, in standardised "***key usage***" attributes, Camerfirma includes "***basic constraints***" marked as critical in the certificate fields and therefore compliance is obligatory by the applications that use it, or limitations on attributes such as "***extended key usage***", "***name constraints***" and/or by means of text included in the "***user notice***" marked "not critical" but for which the certificate holder and user's compliance are obligatory.

## *1.5 Policy Authority*

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

The Certification Authority's activity may be subject to inspection by the Policy Authority (PA) or anyone appointed by it.

For the hierarchies described herein, the Policy Authority falls to Camerfirma's legal department.

Camerfirma's legal department therefore constitutes the Policy Authority for the Hierarchies and Certification Authorities described above and is responsible for managing the CPS.

### 1.5.1 Organization administering the document

The drafting and control of this CPS is managed by the CA Camerfirma SA legal department in collaboration with the operations department.

### 1.5.2 Contact Person

| | |
|---|---|
| **Address:** | Calle Ribera del Loira, 12. Madrid (Madrid) |
| **Phone:** | +34 902 361 207 |
| **Fax:** | +34 902 930 422 |
| **E-mail:** | juridico@camerfirma.com |

In terms of the content of this CPS, it is assumed that the reader is familiar with the basic concepts of PKI, certification and digital signing. Should the reader not be familiar with these concepts, information can be obtained from Camerfirma's website http://www.camerfirma.com where general information can be found about the use of the digital signatures and digital certificates.

To report security incidents related to certificates by the TSP, you can contact AC Camerfirma through **incidentes@camerfirma.com**

### 1.5.3 Person determining CPS suitability for the policy

The legal department of Camerfirma is therefore constituted in the Policy Authority (PA) of the Hierarchies and Certification Authorities described above being responsible for the administration of the CPS.

### 1.5.4 CPS approval procedures

The publication of the revisions of this CPS must be approved by the Management of Camerfirma.

AC Camerfirma publishes every new version on its website. The CPS is published in PDF format electronically signed with the digital certificate of the legal entity of AC Camerfirma SA.

## *1.6 Definitions and Acronyms*

### 1.6.1 Acronyms

| | |
|---|---|
| **CA** | Certification Authority |
| **CPS** | Certification Practice Statement. |
| **CRL** | Certificate Revocation List. List of revoked certificates |
| **CSR** | Certificate Signing Request. |
| **DES** | Data Encryption Standard. Standard for encrypting data |
| **DN** | Distinguished Name. Distinguished name in the digital certificate |
| **DSA** | Digital Signature Algorithm. The signature’s algorithm standard |

| | |
|---|---|
| **FIPS** | Federal Information Processing Standard Publication |
| **IETF** | Internet Engineering Task Force |
| **ISO** | International Standards Organisation International Standards Organisation |
| **ITU** | International Telecommunications Union. |
| **LDAP** | Lightweight Directory Access Protocol. Protocol for directory access |
| **OCSP** | On-line Certificate Status Protocol. Protocol for accessing the status of certificates |
| **OID** | Object Identifier. |
| **PA** | Policy Authority. |
| **PC** | Certification Policy |
| **PIN** | Personal Identification Number. |
| **PKI** | Public Key Infrastructure. |
| **RA** | Registration Authority |
| **RSA** | Rivest-Shamir-Adleman. Type of encryption algorithm |
| **SHA** | Secure Hash Algorithm. |
| **SSCD** | Secure Signature Creation Device |
| **SSCDSD** | Secure Signature Creation Data Storage Device |
| **SSL** | Secure Sockets Layer. A protocol designed by Netscape that has become standard on the Internet. It allows the transmission of encrypted information between a browser and a server. |
| **TCP/IP** | Transmission Control. *Protocol/Internet Protocol*. System of protocols, as defined in the IETF framework. The TCP protocol is used to split source information into packets and then recompile it on arrival. The IP protocol is responsible for correctly directing the information to the recipient. |

### 1.6.2 Definitions

**Activation data**

Private data such as PINs or passwords used for activating the private key

**Applicant**

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

**Certificate**

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

**Certification Authority**

This is the entity responsible for issuing and managing digital certificates. It acts as the trusted third party between the Subject/Signatory and the User Party, associating a specific public key with a person.

**Certification Policy**

A set of rules defining the applicability of a certificate in a community and/or in an application, with common security and usage requirements.

**CPS**

Defined as a set of practices adopted by a Certification Authority for issuing certificates in compliance with a specific certification policy.

**CRL**

A file containing a list of certificates that have been revoked for a certain period of time and which is signed by the CA.

**Cross certification**

Establishing a trust relationship between two CAs, by exchanging certificates between the two under similar levels of security.

**Digital signature**

The result of the transformation of a message, or any type of data, by the private application in conjunction with known algorithms, thus ensuring:

a) that the data has not been modified (integrity)

b) that the person signing the data is who he/she claims (ID)

c) that the person signing the data cannot deny having done so (non-repudiation at origin)

**Entity**

Within the context of these certification policies, a company or organisation of any type with which the applicant has any kind of relationship.

**Key pair**

A set consisting of a public and private key, both related to each other mathematically.

**OID**

A unique numeric identifier registered under the ISO standardisation and referring to a particular object or object class.

**PKI**

A set of hardware, software and human resources elements and procedures, etc., that a system is made up of based on the creation and management of public key certificates.

**Policy authority**

A person or group of people responsible for all decisions relating to the creation, management, maintenance and removal of certification and CPS policies.

**Private key**

A mathematical value known only to the Subject/Signatory and used for creating a digital signature or decrypting data. Also called **signature creation data**.

**Public key**

A publicly known mathematical value used for verifying a digital signature or encrypting data. Also called **signature verification data**.

The CA's private key is to be used for signing certificates and CRLs.

**Registration Authority**

The entity responsible for managing applications and identification and registration of certificates.

**SCDSD**

*Secure Signature Creation Data Storage Device* A software or hardware element used to safeguard the Subject/Signatory's private key so that only he/she has control over it.

**SSCD**

Secure Signature Creation Device. A software or hardware element used by the Subject/Signatory for generating digital signatures, so that cryptographic operations are performed within the device and control is guaranteed solely by the Subject/Signatory.

**Subject/Signatory**

Within the context of this certification practices statement, the natural person whose public key is certified by the CA and who has a valid private key for generating digital signatures.

**User Party**

Within the context of this certification policy, the person who voluntarily trusts the digital certificate and uses it as a means for accrediting the authenticity and integrity of the signed document.

# 2 Publication and Repository Responsibilities

## *2.1 Repository*

Camerfirma provides a service for consulting issued certificates and revocation lists. These services are available to the public on its website: http://www.camerfirma.com/area-de-usuario/consulta-de-certificados/

Query services are designed to ensure availability 24 hours a day, seven days a week.

Policy and certification practice repository. These services are available to the public on its website.

This information is stored in a relational database with security measures to ensure it is stored in accordance with the corresponding Certification Policy requirements.

Camerfirma publishes the issued certificates, revocation lists, and certification policies and practices at no cost.

Camerfirma previously claims authorisation of the certificate holder before publication of the certificate.

## *2.2 Publication*

### 2.2.1 Publication of CA information.

Camerfirma generally publishes the following information in its repository:

- An updated certificate directory indicating the certificates issued and whether they are valid or their application has been suspended, or terminated.
- The lists of revoked certificates and other information about the status of revoked certificates.
- The general certification policy and, where appropriate, specific policies.
- Certificate profiles and lists of revoked certificates.
- The Certification Practices Statement and the corresponding PDS (*PKI Disclosure Statement*).
- Binding legal instruments with Signatories and verifiers.

Any changes to specifications or conditions of service shall be communicated to users by the Certification Authority, through its website http://www.camerfirma.com

AC Camerfirma shall not remove the previous version of the changed document, indicating that it has been replaced by the new version.

External Subordinate CA certificates are published in a repository provided by AC Camerfirma, or if applicable, in its own repository which, by contractual agreement, Camerfirma can access.

#### 2.2.1.1 Certification Policies and Practices.

This CPS and Policies are available to the public on the following website: https://policy.camerfirma.com.

Subordinate CA certification policies are also published or referenced on AC Camerfirma's website.

#### 2.2.1.2 Terms and conditions.

Users can find the service terms and conditions in Camerfirma's certification policies and practices. The Subject/Signatory receives information on the terms and conditions in the certificate issuing process, either via the physical contract or the condition acceptance process prior to submitting the application.

When the Subject/Signatory accepts the terms and conditions on paper they must be signed in writing. If they are accepted in electronic format it is done by accepting the terms and uses in the application form.

#### 2.2.1.3 Distribution of the certificates.

The issued certificates can be accessed as long as the Signatory/Subject has provided consent. Prior to issuing the certificate, the applicant must accept the uses, granting Camerfirma the right to publish the certificate on the website:

http://www.camerfirma.com/area-de-usuario/consulta-de-certificados/.

The root keys in the Camerfirma hierarchies can be downloaded from:
https://www.camerfirma.com/clavespublicas

The certificates can be viewed from a secure website by entering the Signatory's email address. If a Signatory with that email address is found, the system displays a page with all the related certificates, whether active, expired or revoked. Therefore, the query service does not allow the mass download of certificates.

## *2.3 Publication frequency*

AC Camerfirma **publishes the final entity's certificates** immediately after they have been issued, provided the Subject/Signatory has given approval.

AC Camerfirma issues and publishes **revocation lists** periodically in accordance with the table shown in the corresponding section of these certification practices: **"CRL issuance frequency"**.

Camerfirma immediately publishes on its website https://policy.camerfirma.com. Any change to the **Policies and the CPS**, maintaining a version log.

AC Camerfirma may withdraw the reference to change on the home page within 15 (fifteen) days from the publication of the new version and insertion into the corresponding deposit. Older versions of documents are kept for a period of at least **fifteen (15) years** and may be consulted by stakeholders with reasonable cause.

## *2.4 Access controls to repositories*

Camerfirma publishes certificates and CRLs on its website. The certificate holder's email address is required to access the certificate directory, and an anti-robot control must be passed to eliminate the possibility of mass searches and downloads.

Access to revocation information and certificates issued by Camerfirma is free-of-charge.

Camerfirma uses reliable systems for the repository, so that:

- The authenticity of the certificates can be checked. The certificate itself through signature of the certification authority guarantees its authenticity.
- Unauthorised persons cannot alter the data. The digital signature of the certification authority protects against manipulation of the data included in the certificate.
- The applicant may or may or not authorise the publication of the certificate in the application process.

# 3 Identification and Authentication

## *3.1 Initial record*

### 3.1.1 Types of names

The Subject/Certificate holder is described by a distinguished name (DN, *distinguished name*, Subject) pursuant to the X.501 standard. The DN field descriptions are shown in each of the certificate profile sheets. It also includes a *"Common Name"* component (CN =).

Profile records can be requested through AC Camerfirma customer support service on 902 361 207 or via the application https://secure.camerfirma.com/incidencias.

The structure and content of the fields of each certificate issued by Camerfirma as well as its semantic meaning are described in each profile record in the certificates.

- **Natural persons:** In certificates corresponding to natural persons, the identification of the Signatory is made up with their full name and tax ID number.
- **Legal entities:** In certificates corresponding to legal entities, this identification is via their corporate name and tax identification.
- **Components or devices:** The **final entity certificates describing components or devices** incorporate an identifying name of the machine or service, in addition to the legal entity that owns the service in the organisation field "O" of the "CN".
  - The structure for **Subordinate CA, TSU, TSA, OCSP** certificates includes at least:
    - A descriptive name that identifies the Certification Authority (CN)
    - The legal entity responsible for the keys (O)
    - The tax ID number of the organisation responsible for the keys (*OrganizationIdentifier*)
    - The country where the company responsible for the keys carries out the activity. (C)
  - Depending on the type of certificate, the **Secure Server** certificate includes the FQDN (*Fully Qualified Domain Name*) domain on which the organisation "O" described in the certificate has ownership and control.

  The ***ROOT*** certificates have a descriptive name that identifies the Certification Authority:

  CHAMBERS OF COMMERCE ROOT – 2016 or
  GLOBAL CHAMBERSIGN ROOT – 2016

  The (O) field contains the name of the organisation responsible from the Certification Authority: AC CAMERFIRMA SA.

### 3.1.2 Need for names to be meaningful

All Distinguished Names must be meaningful, and the identification the attributes associated to the subscriber should be in a human readable form. See 7.1.4 Name Format

### 3.1.3 Pseudonyms

The acceptance or not of pseudonyms is dealt with in each certification policy. If they are allowed, Camerfirma will use the Pseudonym with the CN attribute of the Subject/Signatory's name, keeping the Subject/Signatory's real identity confidential.

The pseudonym in certificates in which it is allowed is calculated in such a way that the real certificate holder is unmistakably identified**.**

### 3.1.4 Rules used to interpret several name formats

Camerfirma complies with the ISO/IEC 9594 X.500 standard.

### 3.1.5 Uniqueness of names

Within a single CA, a Subject/Signatory name that has already been taken cannot be re-assigned to a different Subject/Signatory. This is ensured by including the unique tax identification code to the name chain distinguishing the certificate holder.

#### 3.1.5.1 Issuance of several natural person certificates for the same certificate holder

Under this CPS, a Signatory may request more than one certificate provided that the combination of the following values in the request is different from a valid certificate:

TAX ID Company tax ID
TAX ID Natural person's tax identifier.
Certificate Type (Certificate Policy Identifier OID).
Certificate media. (Software, Card, Cloud)

As an exception, this CPS can issue a certificate when the Corporate Tax ID No., Personal Tax ID No., type or media matches an active certificate, provided there is a differentiating factor between them in the position (*title*) and/or department (*organizationalUnit*) fields.

### 3.1.6 Recognition, authentication and function of registered trademarks and other distinctive symbols

Camerfirma does not assume any obligations regarding issuing certificates in relation to the use of trademarks or other distinctive symbols. Camerfirma deliberately does not allow the use of a distinctive sign on the Subject/Signatory that does not hold usage rights. However, Camerfirma is not required to seek evidence about the rights to use trademarks or other distinctive signs prior to issuing certificates.

### 3.1.7 Name dispute resolution procedure

Camerfirma is not liable in the case of name dispute resolution. In any case, names are assigned in accordance with the order in which they are entered.

Camerfirma shall not arbitrate this type of dispute, which the parties must settle directly between themselves.

Camerfirma complies with section 2.4.4 of this CPS.

## *3.2 Initial Identity Validation*

Identity verification does not differentiate between certificates in different hierarchies, it is associated with the type of certificate issued.

To properly identify the Applicant's identity, the entity and their relationship, Camerfirma establishes the following requirements through the RA:

### 3.2.1 Methods of proving private key ownership.

Camerfirma uses various circuits for issuing certificates in which the private key is managed differently. Either the user or Camerfirma can create the private key.

The key creation method used is shown in the certificate, through the Policy ID and the Description attribute in the certificate DN field. These codes are described in the corresponding policies and in the certificate profile records.

a) Keys created by Camerfirma.

   **In software:** They are given to the Signatory in person or by mail via protected files, using Standard **PKCS#12**. The security process is guaranteed because the access code to the file **PKCS#12** that enables its installation in applications is delivered by a different method to that used for receiving the file (email, phone).

   **In Hardware:** The keys can be delivered by Camerfirma to the Subject/Signatory, directly or through a registration authority on a qualified signature creation device (QSCD).

b) Keys created by the Signatory.

   The Signatory has a key creation mechanism, either software or hardware. Proof of ownership of the private key in this case is the request that Camerfirma receives in **PKCS#10** format.

### 3.2.2 Entity's ID

Prior to the issuance and delivery of an organisation certificate, data relating to the incorporation and legal status of the entity must be authenticated. The RA requests the required documentation depending on the type of entity in order to identify it. This information is published in the RA's operating manuals and on Camerfirma's website.

http://www.camerfirma.com/index/buscador-documentos.php

For entities outside of Spanish territory, the documentation that must be provided is that of the Official Registrar of the country concerned, duly apostilled where the existence of the entity in that country is indicated.

In the issuance of OV/EV SSL component certificates, the existence of the entity can be checked by accessing the following public registries (www.registradores.org; www.rmc.es), Camerdata (www.camerdata.es), Informa (www.informa.es) or the Spanish Tax Office databases (www.aeat.es). EV must incontrovertibly verify the entity's activity. This is checked by accessing the commercial registry or other business activity registers. For entities outside of Spanish territory, the documentation that must be provided is that of the Official Registrar of the country concerned, duly apostilled where the existence of the entity in that country is indicated. In addition:

- It must be checked that the submitted data or documents are not older than **one year**.
- That the organisation has legally existed for a minimum of **one year**.
- Certificates cannot be issued for eliminated companies in countries where there is a government ban on doing business.

**In Public administrations:** The documentation proving that the public administration, public body or public entity exists is not required because this identity is part of the General State Administration or other State Public Administration's corporate scope.

### 3.2.3 Subject/Signatory Identification

The Subject or Signatory natural person (or alternatives as described in the eIDAS) when this person is also the Applicant, or the Applicant's representative when it is a legal entity, is required to present one of the following documents:

- National Identity Document.
- Residence card.
- Passport.
- Apostille for identification documents of applicants outside of Spanish territory.

Physical presence is not required for these certificates in the cases established in eIDAS.

http://www.camerfirma.com/index/buscador-documentos.php

In the case of a representative of the Subject/Signatory, submission of an authorisation signed by a representative of the entity, who will act as the Applicant. For entities outside of Spanish territory, the document accrediting the representative capacity of the person signing the authorisation shall be issued duly apostilled, to verify the accuracy of the documentation.

#### 3.2.3.1 Proof of relationship

| Certificate type | Documentation |
|---|---|
| Legal Entity Representative with general powers of representation<br>Representative of an entity without legal status with general powers of representation.<br>Legal Entity Representative for procedures with the Public Administrations<br>Representative of a Non-legal Entity for procedures with the Public Administrations<br>Legal Entity Representative for Legal Representatives<br>Representative of a Non-Legal Entity for Legal Representatives | Evidence on the Subject/Signatory's representation powers with respect to the entity, by providing documentation showing their powers of representation depending on the type of entity. This information is published in the RA's operating manuals and on Camerfirma's website. |
| Corporate | Usually, an authorisation signed by the entity's Legal Representative. |
| | |

| Certificate type | Documentation |
|---|---|
| Digital Seal | Authorisation to request the certificate by someone with sufficient power of representation for the signing entity.<br>Certificate or query from the Companies Registry to check the incorporation and legal status of the entity and the appointment and term of office of the authorising person. |
| Public employee/Office and Seal | The identity document of the person who is acting on behalf of the Public Administration, public body or entity is required. The responsible Applicant/person shall be identified by the RA with his/her ID and authorisation from the responsible person, indicating that it is a public employee or appointment in the Official State Gazette where this person's Tax ID No. appears. |

| Certificate type | Documentation |
|---|---|
| Server | Domain control by the Signatory entity. Camerfirma checks that the data found in the WHOIS Internet service match the entity’s information submitted in the request.<br>It may be that the domain is assigned in the registrar’s database to a third party responsible for its management. In this case, the following is required so that the data of the last owner of the domain appears in the certificate:<br>1. An authorisation for issuing the certificate.<br>2. A communication from the organisation or person who controls the domain registration indicating this circumstance.<br>For EV certificates, the certificate issuance guidelines require a distinction to be made between different types of organisations (private, government, business). In these cases, the applicant specifies the type of entity to which he/she belongs on the application form. The registration authority checks that the information is accurate. The certificate includes this information as defined in the reference certification policies.<br>The certificates issued with SAN (Subject Alternative Name) extension. The above procedures should be carried out for each of the domains included in the certificate. The certificate cannot be issued if any of them do not meet established requirements. |

| Certificate type | Documentation |
|---|---|
| CodeSign | Authorisation to request the certificate by someone with sufficient power of representation for the signing entity.<br>Certificate or query from the Companies Registry to check the incorporation and legal status of the entity and the appointment and term of office of the authorising person. |
| TSU | Authorisation to request the certificate by someone with sufficient power of representation for the signing entity.<br>Certificate or query from the Companies Registry to check the incorporation and legal status of the entity and the appointment and term of office of the authorising person. |

#### 3.2.3.2 Service or Machine Identity

The existence of the domain or IP address. This is checked by accessing the WHOIS Internet domains. The use of a domain name or private IP addresses is allowed but obsolete (and will be prohibited after October 2016, which is why Camerfirma stopped issuing certificates of this kind from **1 November 2016**. In any case, issued certificates of this type are revoked if their expiry date is after **October 2016**). The customer is notified of this before the certificate is issued.

Domain information is taken from the WHOIS service of the registrar of the domain for which the rules established in the ccTLD or gTLD are applied. Checked by accessing the WHOIS Internet domains:

- http://www.internic.net/whois.html
- http://www.networksolutions.com
- http://en.gandi.net
- http://www.interdomain.es
- https://www.nic.es (.es domains)
- http://www.eurid.eu (.eu domains)
- http://www.nic.coop/whoissearch.aspx (.coop domains)
- http://www.nominalia.com
- http://www.arsys.es

Camerfirma notify the domain contact, sending a random value by email and then receiving a confirming response utilizing the Random Value.

When the request for issuance is for a secure server or digital office certificate, PKI Platform will examine the registration of the authorised CAs, CAA, pursuant to RFC 6844, and if those CAA records are present and do not allow Camerfirma to issue those certificates because they are not registered, Camerfirma will not issue such a certificate. Camerfirma will allow applicants to re-submit the application once this situation has been solved. The customer must modify his/her domain's data to allow Camerfirma to issue such a certificate.

Camerfirma use the following label in the DNS CAA record “issue” “issewild”:

**“camerfirma.com”**

#### 3.2.3.3 User identification considerations for senior management roles.

Camerfirma uses special procedures for identifying senior management positions in companies and administrations for issuing digital certificates. In these cases, a registry operator goes to the organisation’s premises to ensure the physical presence of the certificate holder. For the relationship between the certificate holder and the organisation represented in public administration, the publication of the positions in official state gazettes is often used.

#### 3.2.3.4 Considerations in identifying users and associations in the public Administration

There are aspects to consider regarding registration authorities in public administration and operated by public employees; the latter are considered notaries to guarantee the relationship between a public employee requesting the certificate and the entity to which he/she is associated. In these cases, compiling the documentation that forms part of the record can be simplified.

### 3.2.4 Non-verified subscriber information

It’s not allowed to include non-verified information in the “Subject Name” of a certificate.

### 3.2.5 In RA operator certificates (natural person)

Firstly, it is checked that the applicant has passed the operator’s examination and secondly that the data is identical to that of the RA operator’s record delivered by the organisation to that which belongs to the operator. The Corporate Tax ID No. is checked to ensure it is associated with the organisation and that the mail associated with the certificate is an email from the organisation.

### 3.2.6 Special considerations for issuing certificates outside of Spanish territory

Aspects related to the identity documentation of natural persons, legal entities and associations between them in the different countries where Camerfirma issues certificates. The documentation required for this is that which is legally applicable in each country provided that it allows for compliance with the obligation of the corresponding identification pursuant to Spanish law.

- PERU
- ANDORRA
- COLOMBIA
- MEXICO
- UK
- FRANCE

## *3.3 Identification and authentication for re-key requests*

### 3.3.1 Identification and authentication for routine re-key

Once a certificate has been rendered invalid, it cannot be renewed automatically. The applicant must start a new issuance procedure.

***Exception**: When the renewal takes place on final entity certificates due to a certificate replacement process or an issuing error or **a loss**, the certificate can be renewed following a revocation, as long as it shows the current situation. The supporting documentation submitted to issue the replaced certificate is reused and the physical presence is no longer required, if this were necessary due to the type of certificate. Camerfirma updates the number of years since the last physical presence to the status of the certificate being replaced, just as if this process had been the result of an ordinary renewal.*

### 3.3.2 Identification and authentication for re-key after revocation

## *3.4 Identification and authentication for revocation request*

The method for submitting revocation requests is established in section 4.8 of this document.

# 4 Certificate life-cycle operational requirements

AC Camerfirma uses its STATUS platform for certificate lifecycle management. This platform allows the application, registration, publication and revocation of all certificates issued.

## *4.1 Certificate request*

### 4.1.1 Who can submit a certificate application

A certificate application can be submitted by the subject of the certificate or by an authorized representative of the subject.

### 4.1.2 Enrollment process and responsibilities

#### 4.1.2.1 Web forms.

Certificate requests are submitted via the application forms at the address or by sending the applicant a link to a specific form.

http://www.camerfirma.com/certificados/

The website contains the forms required to apply for each type of certificate that Camerfirma distributes in different formats and the signature creation devices, if they are required.

The form allows for the inclusion of a CSR (PKCS#11) if the user has created the keys.

After confirmation of the application data, the user receives an email sent to the account associated with the certificate application containing a link to confirm the application and accept the terms of use.

Once the application is confirmed, the Signatory is informed of the documentation to be submitted in a registry office for this purpose and to comply with the physical identification requirement, if applicable.

Applications for Subordinate CA and TSA certificates must be made formally through the application for a sales quotation and be subsequently incorporated into the application forms on the STATUS platform.

#### 4.1.2.2 Batches.

The STATUS platform also allows batch request circuits. In this case, the applicant sends the RA a file with a structure designed by Camerfirma containing the applicants' details. The RA uploads these requests in the management application.

#### 4.1.2.3 Applications for final-entity certificates in HSM, TSU and Subordinate CA.

Applications for issuing certificates in HSM, TSU or Subordinate CA are made through a sales quotation at a sales area. http://www.camerfirma.com/camerfirma/localizacion.

AC Camerfirma reserves the right to send an internal or external auditor to verify that the development of the key creation event complies with certification policies and associated practices.

When the customer generates the cryptographic keys in an HSM device using its own resources and requests a certificate on hardware, Camerfirma collects the necessary evidence, for which it requests the following documents:

- Statement from the applicant indicating that the keys have been generated within a hardware device and/or a technical report from a third party (service provider) certifying this process. AC Camerfirma provides the statement forms for Signatories and third parties.

- Records from key creation events indicating:

    - The process followed to create the keys
    - The people involved
    - The environment in which it was created
    - The HSM device used (model and make)
    - Security policies employed: (size of keys, key creation parameters, exportable/not exportable and any other relevant information)
    - The PKCS#10 request generated
    - Any incidents and solutions.

- Device specifications: The technical data sheet of the devices may be acceptable.

This information is included by the RA into the media documentary record for issuing the certificate.

For each type of certificate, the Signatory must accept the terms and conditions of use between the Signatory, the registration authority and the certification authority. This is carried out by manually signing a contract or accepting the terms and conditions displayed on a website before creating and downloading the certificate.

#### 4.1.2.4 Applications via Web Services (WS) layer.

In order to integrate third party applications in the Camerfirma certificate management platform, a Web Services (WS) layer has been created that provides certificate issuance, renewal and revocation services. Calls to these WS are signed with a certificate recognised by the platform.

The “blind” issuance of such certificates means that the process is reviewed in detail. Before beginning the issuance by means of this system, there must be a favourable Camerfirma technical report, a contract where the registration authority agrees to maintain the system in optimum security conditions and to notify Camerfirma of any change or incident. In addition, the system is subject to annual audits to verify the following:

1. Documentary records of certificates issued
2. That the certificates are being issued under the guidelines established by the certification policies and this certification practices statement under which they are governed.

#### 4.1.2.5 Cross certification request

Camerfirma does not have any cross certification process established at this time.

## *4.2 Processing the certification request.*

### 4.2.1 Performing identification and authentication functions

Once a certificate has been requested, the RA operator, by means of access to the management platform (STATUS), shall verify that the information provided is consistent.

The operator of the platform has an internal management certificate issued for these operations and that is obtained after a training and evaluation process.

The certificate used by the registry operator is considered a multi-factor access used not only for access to the PKI management platform (STATUS) but also to approve each request for issuance of a certificate by making an electronic signature

### 4.2.2 Approval or rejection of certificate applications

The registry operator views the requests pending processing and those that have been assigned.

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

If the information is not correct, the RA rejects the request. If the data is verified correctly, the Registration Authority approves issuance of the certificate by means of digital signature with its operator certificate.

### 4.2.3 Time to process certificate applications

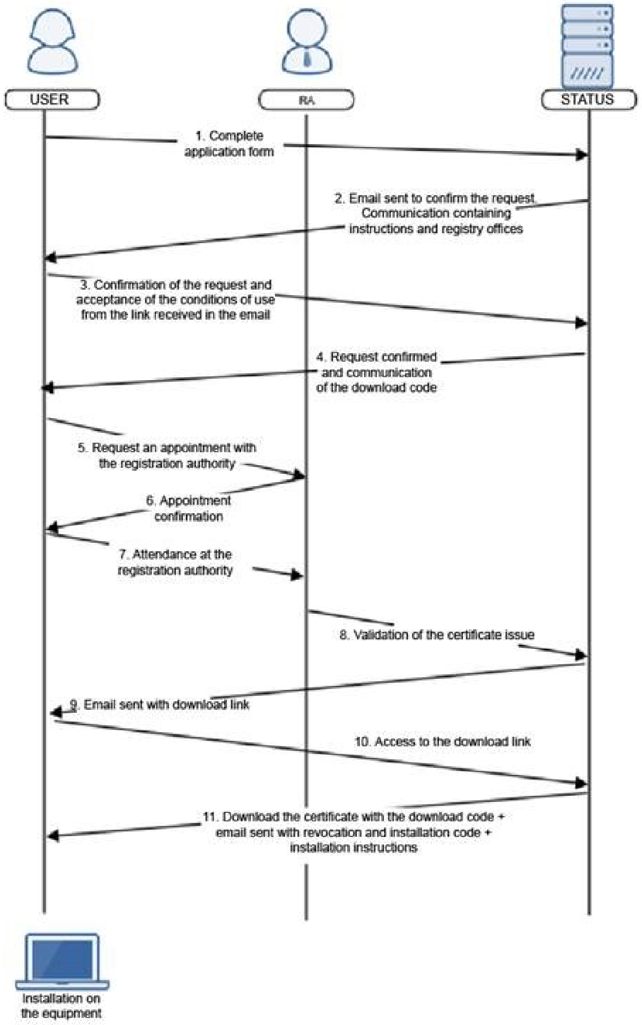
Applications via web services are processed as soon as they are received authenticated with a certificate previously recognised by Camerfirma.

## *4.3 Certificate issuance*

### 4.3.1 CA actions during certificate issuance

#### 4.3.1.1 Certificates via Software:

Once the application is approved, the Signatory receives an email with notification of this fact and can generate and download the certificate. The product code provided with the contract and an installation code sent in a separate email together with a revocation code is required to install it.

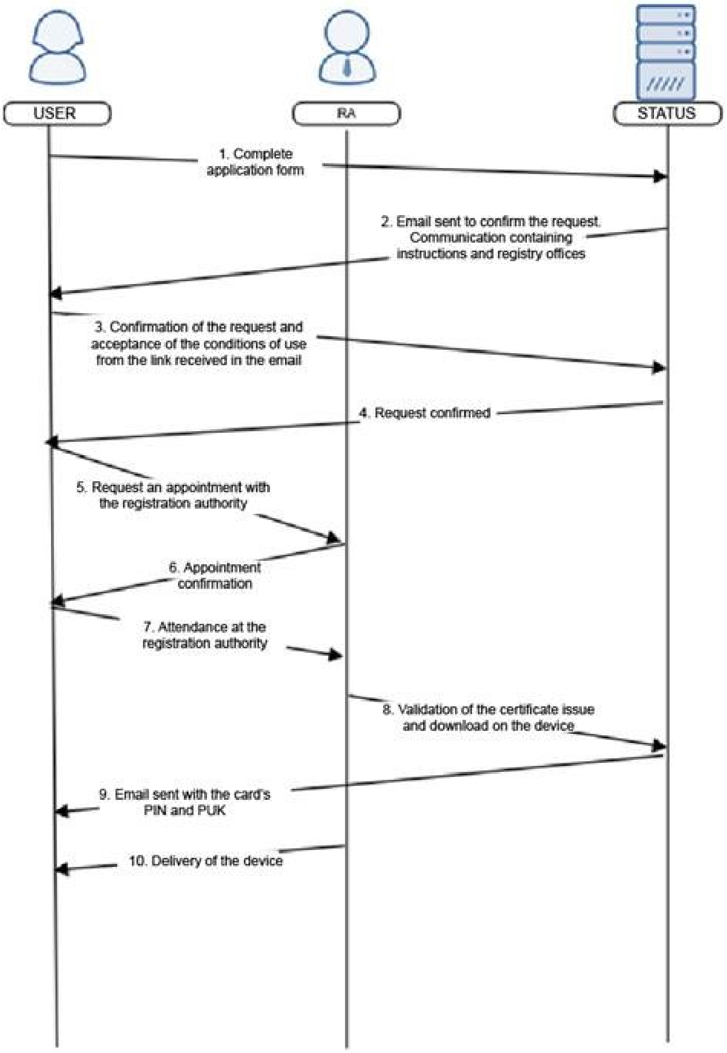


USER
RA
STATUS
1. Complete application form
2. Email sent to confirm the request. Communication containing instructions and registry offices
3. Confirmation of the request and acceptance of the conditions of use from the link received in the email
4. Request confirmed and communication of the download code
5. Request an appointment with the registration authority
6. Appointment confirmation
7. Attendance at the registration authority
8. Validation of the certificate issue
9. Email sent with download link
10. Access to the download link
11. Download the certificate with the download code + email sent with revocation and installation code + installation instructions
Installation on the equipment

Reference document: **IN-2008-03-01**-Generation_certs_software

#### 4.3.1.2 Certificates via HW (Secure Signature Creation Device):

##### *4.3.1.2.1 Cryptographic Card or Token.*


USER
RA
STATUS
1. Complete application form
2. Email sent to confirm the request. Communication containing instructions and registry offices
3. Confirmation of the request and acceptance of the conditions of use from the link received in the email
4. Request confirmed
5. Request an appointment with the registration authority
6. Appointment confirmation
7. Attendance at the registration authority
8. Validation of the certificate issue and download on the device
9. Email sent with the card's PIN and PUK
10. Delivery of the device

The user receives the signature device with the certificates and keys at the RA's offices.

The Registration Authority operator chooses which security card to use to create the keys. For this purpose, the operator's work station is configured with the CSP (Cryptographic Service Provider). AC Camerfirma currently allows several types of USB cards and tokens, all SSCD certified (Secure Signature Creation Device).

For cards by default (sent by Bit4Id) the Signatory receives the cryptographic device access code and unlocking code, as well as a revocation key, via the associated email account. Other PIN/PUK management cards are outside of the scope of this document.

***4.3.1.2.2 Requests via WS:*** *Requests can be received via duly signed calls to the STATUS application WS services layer pursuant to section 4.1.4.*

### 4.3.1.3 EV Secure server certificate

In accordance with the specific policies for EV secure server certificates, these certificates require the physical presence of the applicant or an approved third party. The RA administrator must verify the service payment, the related documentation and the Subject/Signatory's identity.

The certification policies for issuing SSL EV certificates to those that adhere to this CPS ("*CA/Browser Forum Guidelines for Issuance and Management of extended validation certificates*"), require that each EV certificate issue request is approved by two different people. The procedure followed to validate these certificates guarantees double verification, as follows:

- Operator validation of the registration of administrative details and physical presence and delivery of documentation and authorisations.

- Once this procedure is complete, the AC Camerfirma internal audit department checks the documentation and proceeds with the final certificate validation and issuance.

Signatories can use their own resources to create the keys in a cryptographic device and deliver the request to Camerfirma in PKCS#10 format to issue the certificate. In the event that the certificate was issued under the HSM hardware device format, evidence of this is requested as described in section 4.1.3 of this document.

If Camerfirma creates the private key, once the RA operator has approved the request, the following is sent to the Subject/Signatory:

- ✓ A link to the web page where the certificate is created in PKCS#12 format.
- ✓ A password is required to install the keys and certificate on the Signatory's computer.
- ✓ The Subject/Signatory also requires a download code supplied by the application during the application process to obtain the keys and certificate.

If the Signatory generates the key, Camerfirma sends the user a certificate in PKCS#7 format.

### 4.3.1.4 Certificates for encryption.

Under these certification practices, encryption-only certificates are issued for high-level Public Administration employees.

#### 4.3.1.5 Subordinate CA Certificates:

Subordinate CA certificates are issued in a Subordinate CA certificate issuance event in AC Camerfirma’s facilities in a secure environment and under the supervision of an internal auditor.

#### 4.3.1.6 TSU certificates:

TSU certificates are issued in a certificate issuing ceremony in a secure environment by trusted personnel.

### 4.3.2 Notification to subscriber by the CA of issuance of certificate

In the final entity certificates issued by Camerfirma, an email notification is sent to the applicant indicating the request's approval or denial.

Intermediate or root entity certificates are issued in a key ceremony and subsequently delivered to the certificate holder.

## *4.4 Certificate acceptance.*

### 4.4.1 Conduct constituting certificate acceptance

Once the certificate has been delivered or downloaded, the user has seven days to verify that it has been issued correctly.

If the certificate has not been issued correctly due to technical problems, it is revoked and a new one is issued.

### 4.4.2 Publication of the certificate by the CA

Certificates issued are published at http://www.camerfirma.com/area-de-usuario/consulta-de-certificados/

Camerfirma distributes its Root certificates on its website:
http://www.camerfirma.com/area-de-usuario/descarga-de-claves-publicas/

Camerfirma issues its Subordinate CA certificates on its website:
http://www.camerfirma.com/area-de-usuario/jerarquia-politicas-y-practicas-de-certificacion/

Camerfirma distributes its OCSP certificates on its website:
http://www.camerfirma.com/servicios/respondedor-ocsp/

Camerfirma distributes its TSA certificates on its website: http://www.camerfirma.com/servicios/sellado-de-tiempo/

### 4.4.3 Notification of the issuance to third parties

AC Camerfirma provides a system for querying the status of certificates issued, on its website http://www.camerfirma.com/area-de-usuario/consulta-de-certificados/. Access to this page is free.

In some cases the national supervisor is required to send the certificates and CRL issued by the provider on a regular basis.

In the case of SSL EV certificates, notification is sent to various accredited registration services prior to issuing the certificate. Google requires this for recognition of SSL EV certificates in a process called **"Certificate Transparency"**.

## *4.5 Key pair and certificate usage*

### 4.5.1 Subscriber private key and certificate usage

The CA makes all reasonable efforts to confirm that the CA's signature keys are used only for the purposes of generating certificates and signing CRLs.

The key usage limitation is defined in the certificate content in the extensions: *keyUsage*, *extendedKeyUsage* and *basicConstraints*

| CA | Key Usage | Extended Key Usage | Basic Constraints |
|---|---|---|---|
| **CHAMBERS OF COMMERCE ROOT – 2016**<br>**CHAMBERS OF COMMERCE ROOT – 2018** | critical, cRLSign, keyCertSign | - | critical,CA:true |
| **AC CAMERFIRMA FOR NATURAL PERSONS - 2016** | critical, cRLSign, keyCertSign | emailProtection<br>clientAuth | critical,CA:true, pathlen:2 |
| Qualified Citizen Certificate | critical, digitalSignature, contentCommitment, keyEncipherment | emailProtection<br>clientAuth | critical,CA:false |
| Qualified Corporate Certificate | critical, digitalSignature, contentCommitment, keyEncipherment | emailProtection<br>clientAuth | critical,CA:false |
| Qualified Certificate for a Legal Entity Representative with general powers of representation | critical, digitalSignature, contentCommitment, keyEncipherment | emailProtection<br>clientAuth | critical,CA:false |
| Qualified Certificate for a Representative of a Non-legal Entity with general powers of representation | critical, digitalSignature, contentCommitment, keyEncipherment | emailProtection<br>clientAuth | critical,CA:false |
| Qualified Legal Entity Representative Certificate for procedures with the Public Administrations | critical, digitalSignature, contentCommitment, keyEncipherment | emailProtection<br>clientAuth | critical,CA:false |

| CA | Key Usage | Extended Key Usage | Basic Constraints |
|---|---|---|---|
| Qualified Certificate for a Representative of a Non-legal Entity for procedures with the Public Administrations | critical, digitalSignature, contentCommitment, keyEncipherment | emailProtection clientAuth | critical,CA:false |
| Qualified Legal Entity Representative Certificate for Legal Representatives | critical, digitalSignature, contentCommitment, keyEncipherment | emailProtection clientAuth | critical,CA:false |
| Qualified Certificate for a Representative of a Non-legal Entity for Legal Representatives | critical, digitalSignature, contentCommitment, keyEncipherment | emailProtection clientAuth | critical,CA:false |
| Qualified Public Employee Signature Certificate. High Level. | critical, contentCommitment | - | critical,CA:false |
| Public Employee Authentication Certificate. High Level. | critical, digitalSignature | emailProtection clientAuth | critical,CA:false |
| Public Employee Encrypted Certificate High Level. | critical, keyEncipherment, dataEncipherment | emailProtection clientAuth | critical,CA:false |
| Public Employee Qualified Certificate. Mid Level. | critical, digitalSignature, contentCommitment, keyEncipherment | emailProtection clientAuth | critical,CA:false |
| Qualified Public Employee Certificate with Signature Pseudonym. High Level. | critical, contentCommitment | - | critical,CA:false |
| Public Employee Certificate with Signature Authentication. High Level. | critical, digitalSignature | emailProtection clientAuth | critical,CA:false |
| Public Employee Certificate with Encrypted Pseudonym. High Level. | critical, keyEncipherment, dataEncipherment | emailProtection clientAuth | critical,CA:false |
| Qualified Public Employee Certificate with Pseudonym. Mid Level. | critical, digitalSignature, contentCommitment, keyEncipherment | emailProtection clientAuth | critical,CA:false |
| **AC CAMERFIRMA FOR LEGAL PERSONS - 2016** | critical, cRLSign, keyCertSign | emailProtection clientAuth | critical,CA:true, pathlen:2 |
| Qualified Digital Seal Certificate | critical, digitalSignature, contentCommitment, keyEncipherment | emailProtection clientAuth | critical,CA:false |
| Digital Seal Certificate | critical, digitalSignature, contentCommitment, keyEncipherment | emailProtection clientAuth | critical,CA:false |
| Public Administrations Digital Seal Certificate. High Level. | critical, digitalSignature, contentCommitment, keyEncipherment | emailProtection clientAuth | critical,CA:false |
| Public Administrations Digital Seal Certificate. Mid Level. | critical, digitalSignature, contentCommitment, keyEncipherment | emailProtection clientAuth | critical,CA:false |
| **AC CAMERFIRMA FOR WEBSITES – 2016**<br>**AC CAMERFIRMA FOR WEBSITES - 2018** | critical, cRLSign, keyCertSign | serverAuth | critical,CA:true, pathlen:2 |
| OV Website Certificate | critical, digitalSignature, keyEncipherment | serverAuth | critical,CA:false |
| Qualified EV Website Certificate | critical, digitalSignature, keyEncipherment | serverAuth | critical,CA:false |
| Qualified Digital Office Certificate - High Level - EV | critical, digitalSignature, keyEncipherment | serverAuth | critical,CA:false |
| Qualified Digital Office Certificate - Mid-level - EV | critical, digitalSignature, keyEncipherment | serverAuth | critical,CA:false |

| CA | Key Usage | Extended Key Usage | Basic Constraints |
|---|---|---|---|
| Qualified Digital Office Certificate - Mid-level - OV | critical, digitalSignature, keyEncipherment | serverAuth | critical,CA:false |
| Qualified Digital Office Certificate - Mid-level - OV | critical, digitalSignature, keyEncipherment | serverAuth | critical,CA:false |
| **AC CAMERFIRMA CODESIGN – 2016** | critical, cRLSign, keyCertSign | codeSigning | critical,CA:true, pathlen:2 |
| Qualified CodeSign Certificate | critical, digitalSignature | codeSigning | critical,CA:false |
| Qualified EV CodeSign Certificate | critical, digitalSignature | codeSigning | critical,CA:false |
| **AC CAMERFIRMA TSA - 2016** | critical, cRLSign, keyCertSign | timeStamping | critical,CA:true, pathlen:2 |
| TSU Qualified Certificate | critical, contentCommitment | critical,timeStamping | critical,CA:false |
| TSU certificate | critical, contentCommitment | critical,timeStamping | critical,CA:false |
| **GLOBAL CHAMBERSIGN ROOT - 2016** | critical, cRLSign, keyCertSign | - | critical,CA:true |
| **AC CAMERFIRMA - 2016** | critical, cRLSign, keyCertSign | - | critical,CA:true, pathlen:2 |
| **AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016** | critical, cRLSign, keyCertSign | emailProtection<br>clientAuth | critical,CA:true, pathlen:1 |
| Citizen certificate | critical, digitalSignature, contentCommitment, keyEncipherment | emailProtection<br>clientAuth | critical,CA:false |
| Corporate certificate | critical, digitalSignature, contentCommitment, keyEncipherment | emailProtection<br>clientAuth | critical,CA:false |
| Legal Entity Representative Certificate | critical, digitalSignature, contentCommitment, keyEncipherment | emailProtection<br>clientAuth | critical,CA:false |
| Non-Corporate Entity Representative Certificate | critical, digitalSignature, contentCommitment, keyEncipherment | emailProtection<br>clientAuth | critical,CA:false |
| **AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016** | critical, cRLSign, keyCertSign | emailProtection<br>clientAuth | critical,CA:true, pathlen:1 |
| Digital Seal Certificate | critical, digitalSignature, contentCommitment, keyEncipherment | emailProtection<br>clientAuth | critical,CA:false |
| **AC CAMERFIRMA GLOBAL FOR WEBSITES - 2016** | critical, cRLSign, keyCertSign | serverAuth | critical,CA:true, pathlen:1 |
| EV Website Certificate | critical, digitalSignature, keyEncipherment | serverAuth | critical,CA:false |
| **AC CAMERFIRMA GLOBAL TSA – 2018** | critical, cRLSign, keyCertSign | timeStamping | critical,CA:true, pathlen:1 |
| Globla TSU Certificate | critical, digitalSignature, keyEncipherment | critical:timeStamping | critical,CA:false |
| **AC CAMERFIRMA COLOMBIA - 2016** | critical, cRLSign, keyCertSign | - | critical,CA:true, pathlen:2 |
| **AC CITISEG - 2016** | critical, cRLSign, keyCertSign | emailProtection<br>clientAuth | critical,CA:true, pathlen:1 |
| Academic Community Certificate | critical, digitalSignature, contentCommitment, keyEncipherment | emailProtection<br>clientAuth | critical,CA:false |
| Public Official Certificate | critical, digitalSignature, | emailProtection<br>clientAuth | critical,CA:false |

| CA | Key Usage | Extended Key Usage | Basic Constraints |
|---|---|---|---|
|  | contentCommitment, keyEncipherment |  |  |
| Legal Entity Certificate | critical, digitalSignature, contentCommitment, keyEncipherment | emailProtection clientAuth | critical,CA:false |
| Natural person certificate | critical, digitalSignature, contentCommitment, keyEncipherment | emailProtection clientAuth | critical,CA:false |
| Contractual Relationship Certificate | critical, digitalSignature, contentCommitment, keyEncipherment | emailProtection clientAuth | critical,CA:false |
| Qualified Professional Certificate | critical, digitalSignature, contentCommitment, keyEncipherment | emailProtection clientAuth | critical,CA:false |
| Company Representative Certificate | critical, digitalSignature, contentCommitment, keyEncipherment | emailProtection clientAuth | critical,CA:false |
| **AC CAMERFIRMA PERU - 2016** | critical, cRLSign, keyCertSign | - | critical,CA:true, pathlen:2 |
| **AC CAMERFIRMA PERU CERTIFICATES - 2016** | critical, cRLSign, keyCertSign | emailProtection clientAuth | critical,CA:true, pathlen:1 |
| Certificate for a natural person linked to a company | critical, digitalSignature, contentCommitment, keyEncipherment | emailProtection clientAuth | critical,CA:false |
| Legal Representative Certificate | critical, digitalSignature, contentCommitment, keyEncipherment | emailProtection clientAuth | critical,CA:false |
| Legal Entity Certificate | critical, digitalSignature, contentCommitment, keyEncipherment | emailProtection clientAuth | critical,CA:false |
| Digital Invoicing Certificate | critical, digitalSignature, contentCommitment, keyEncipherment | emailProtection clientAuth | critical,CA:false |
| Physical Person Certificate (Certificates for individuals) | critical, digitalSignature, contentCommitment, keyEncipherment | emailProtection clientAuth | critical,CA:false |
| Electronic Invoice Certificate (Certificates for natural persons) | critical, digitalSignature, contentCommitment, keyEncipherment | emailProtection clientAuth | critical,CA:false |

*Although data encryption with certificates is technically possible, Camerfirma is not responsible for any resulting damages should the holder not be able to retrieve the private key required to decipher the information, except in the certificate issued solely for this use.*

### 4.5.2 Relying party public key and certificate usage

Relying parties must access and use the public key and certificate as stipulated in this CPS and as indicated in the “Relying Party Agreement”.

## *4.6 Certificate renewal.*

### 4.6.1 Circumstance for certificate renewal

**Subordinate CA** certificates are not renewed automatically; they must be issued in a new procedure based on prior planning, ensuring that the life of the certificate is always longer than the maximum validity period of certificates issued under its hierarchical branch.

**RA Operator** certificates are renewed every year as long as there is no proof that the entity has ceased to be an RA operator.

**TSU** certificates are issued for a period of six years with a private key use of one year, which are renewed annually.

**ROOT** certificates are issued in a new procedure through a process created for this purpose.
**OCSP** certificates are issued periodically and no renewal processes are established.

### 4.6.2 Who may request renewal

In certificates where renewal is allowed, the holder is authenticated on the basis of the certificate to be renewed.

### 4.6.3 Processing certificate renewal requests

Before renewing a certificate, Camerfirma checks that the information used to verify identity and other data of the Signatory and the key holder is valid.

Under these practices, if any of the Signatory or key holder’s information has changed, a new record must be made and issued pursuant to the relevant sections in this document.

*Camerfirma always issues new keys to renew certificates. Therefore, the technical process of issuing the certificate is the same as the process for submitting a new application.*

In the case of renewal of **qualified certificates of a natural person's final entity**, the certificate can be issued without physical presence up to a period of **five years** from the last record of physical presence. Once the established period has lapsed, the Signatory must repeat the same physical issuance process as for the first issuance. Under these practices, if five years has not transpired at the time the certificate is renewed, the certificate holder's physical presence is not required.

Camerfirma gives the Signatory four warnings that the certificate is about the expire (30 days, 15 days, seven days, one day) via email.

The renewal process can be initiated from the Camerfirma website http://www.camerfirma.com/area-de-usuario/renovacion-de-certificados/. A valid (not revoked) certificate is required to complete the renewal process.

- Once the certificate being renewed has been identified, the application gives the Signatory the old certificate details and requests confirmation. The application allows the Signatory to change the email address assigned to the certificate. If other information included in the certificate has changed, the certificate must be revoked and a new one issued.

- The request is included in the RA application. Once the operator has checked the data, the CA is requested to issue the certificate.

- As a general rule, Camerfirma issues a new certificate, taking the expiry date of the certificate being renewed as this new certificate's start date. In some cases, certificate renewal with the date at the same time of renewal, subsequently revoking the certificate to be renewed, is allowed in the emission processes through web services.

*Technical certificates (secure server, corporate seal and CodeSign) cannot be renewed; the process for issuing a new certificate must be followed.*

### 4.6.4 Notification of new certificate issuance to subscriber

The notification of the issuance of a renewed certificate it will occur as described in section 4.3.2 of this document.

### 4.6.5 Conduct constituting acceptance of a renewal certificate

As stipulated in section 4.4.1 of this document.

### 4.6.6 Publication of the renewal certificate by the CA

As stipulated in section 4.4.2 of this document.

### 4.6.7 Notification of certificate issuance by the CA to other entities

No stipulation

## *4.7 Key Renewal*

This is the usual procedure for renewing Camerfirma certificates, by which all the processes described in this section refer to this renewal method. Camerfirma does not allow certificate renewal without key renewal.

## *4.8 Certificate modification*

Any need for modification to certificates requires a new application. The certificate is revoked and a new one issued with the corrected data.

If it is a certificate **replacement process**, it is considered to be a renewal and thus counted when calculating the years of renewal without physical presence as required by law.

The certificates may be modified as renewal when the attributes of the Signatory or key holder that form part of the uniqueness control provided for this policy have not changed.

If the modification request is made within the ordinary period for renewal of the certificate, it is renewed instead of modified with prior revocation of the certificate to be modified.

## *4.9 Certificate suspension and revocation.*

Revocation refers to any change in a certificate's status caused by being rendered invalid due to any reason other than its expiry.

Suspension, on the other hand, refers to revocation with cause for suspension (i.e. a specific revocation case). A certificate is revoked until it is decided whether it should be revoked definitively or activated.

Rendering a digital certificate invalid due to revocation or suspension becomes effective for third parties as soon as notice of the termination has been given in the certification service provider's certificate validity query service (publication of the list of revoked certificates or query the OCSP service).

The reasons for suspending a certificate are defined in the specific certification policy.

***AC Camerfirma maintains the certificates on the revocation list until the end of their validity. When this occurs, they are removed from the list of revoked certificates.*** *Camerfirma will only eliminate a certificate from the revocation list in either of the following situations:*

- Certificate expired

- Certificate revoked due to suspension, and once reviewed it is concluded that there are no reasons for it to be revoked definitively.

However, Camerfirma maintains the information about the status of an expired certificate in its databases and it can be accessed via the OCSP service.

Revoked certificates cannot be reinstalled under these practices.

The OCSP response for a revoked certificate when it expires maintains the revoked status and its cause.

Due to the different natures of the OCSP and CRL services, in the case of obtaining different responses for an expired certificate, the response given by the OCSP shall be maintained as a valid response.

For Camerfirma, the consultation service for the status of a primary certificate is the one offered by OCSP.

### 4.9.1 Causes for revocation and documentary proof

The reasons for revoking a certificate are defined in the specific certification policy.

As a general rule, a certificate will be revoked where:

- Any of the details contained in the certificate are amended.
- Errors or incomplete data detected in the data submitted in the certificate request or there are changes to the circumstances verified for issuing the certificate.
- Failure to pay for the certificate.

Due to circumstances affecting key or certificate security.

- The private key or infrastructures or systems belonging to the Certification Authority that issued the certificate are compromised, whenever this incident affects the accuracy of the issued certificates.
- The Certification Authority has breached the requirements in the certificate management procedures established in this CPS.
- The security of the key or certificate belonging to the Signatory or person/entity responsible for the certificate is compromised or suspected of being compromised.
- There is unauthorised third party access or use of the private key of the Signatory or person/entity responsible for the certificate.
- There is misuse of the certificate by the Signatory or person/entity responsible for the certificate or failure to keep the private key secure.

Due to circumstances affecting the security of the cryptographic device

- Security of the cryptographic device is compromised or suspected of being compromised.
- There is loss or disablement due to damage to the cryptographic device.
- There is unauthorised third party access to the activation details of the Signatory or person/entity responsible for the certificate.

There are circumstances that affect the Signatory or person/entity responsible for the certificate.

- The relationship is terminated between the Certification Authority and the Signatory or person/entity responsible for the certificate.
- There are changes to or termination of the underlying legal relationship or cause for issuing the certificate to the Signatory or person/entity responsible for the certificate.
- The applicant breaches part of the requirements established for requesting the certificate.
- The Signatory or person responsible for the certificate breach part of their obligations, responsibility and guarantees established in the legal document or in this Certification Practices Statement.
- The sudden incapacity or death of the Signatory or person/entity responsible for the certificate.
- There is a termination of the legal entity that is Signatory of the certificate and expiry of the authorisation provided by the Signatory to the person/entity responsible for the certificate, or termination of the relationship between the Signatory and the person/entity responsible for the certificate.
- The Signatory requests revocation of the certificate in accordance with the provisions of this CPS.
- Firm resolution of the competent administrative or judicial authority

Other circumstances

- Suspension of the digital certificate for a longer period than established in this CPS.
- Termination of the Certification Authority’s service, in accordance with the corresponding section of this CPS.

In order to justify the need for the proposed revocation, required documents must be submitted to the RA or CA, depending on the reason for the request.

- If the certificate holder or the natural person applying for the certificate for a legal entity, a signed statement must be provided indicating the certificate to be revoked and the reason for this request and identification must be provided to the RA.

- If the revocation is requested by a third party, it must present authorisation from the natural person certificate holder or the legal representative of the legal entity certificate holder. The third party must indicate the reasons for requesting revocation of the certificate and identify itself to the RA.

- If the entity requesting revocation is associated with the certificate holder due to termination of the relationship with it, this circumstance must be proven (revocation of powers, contract termination, etc.) and they applicant must identify him/herself to the RA as authorised to represent the entity.

The Signatories have revocation codes that they can use in the online revocation services or by calling the helplines.

### 4.9.2 Who can request revocation

Certificate revocation can be requested by:

- The Subject/Signatory
- The responsible Applicant
- The Entity (via a representative)
- The RA or CA.

Anyone established in the specific certification policies.

### 4.9.3 Revocation request procedure.

All requests must be made:

- ✓ Via the online Revocation Service, by accessing the revocation service on Camerfirma's website and entering the Revocation PIN number.

  http://www.camerfirma.com/area-de-usuario/revocacion-de-certificados/

- ✓ By physically going to the RA's offices during opening hours, showing the Subject/Signatory or Applicant's National Identity Card.
- ✓ By sending Camerfirma a document signed by a representative with sufficient representation powers for the entity requesting certificate revocation. This form must be used to revoke Subordinate CA and TSU certificates.
- ✓ For **secure server, corporate seal or CodeSign** certificates, this revocation can be requested by email, using the address used to request issuance of the certificate, sending the revocation request to gestión_soporte@camerfirma.com. The Camerfirma operator must confirm the revocation request by telephone in order to act upon it.

Camerfirma stores all the information relating to certificate revocation processes on its website.

http://www.camerfirma.com/area-de-usuario/revocacion-de-certificados/

***The revocation management service and the query service are considered critical services, as specified in Camerfirma's contingency plan and business continuity plan**. These services are available **24 hours a day, seven days a week**. In the event of a system failure, or any other circumstance out of Camerfirma's control, Camerfirma will make every effort to ensure that services are not down longer than **24 hours**.*

In case of revocation due to non-payment of the issued certificate price, the RA or CA shall request by emailing the Signatory at their contact e-mail address, prior and on two successive occasions, that this situation is remedied within **eight days**, failing which, the certificate will be revoked immediately.

### 4.9.4 Revocation period

**For final-entity certificates**. The revocation period, from the moment Camerfirma or an RA has reliable knowledge of a certificate revocation, takes place immediately, and is included in the next CRL issued and based on the data from the management platform from which the OCSP responder is fed.

### 4.9.5 Time within which CA must process the revocation request

Camerfirma will process a revocation request immediately following the procedure described in point 4.9.3

In the revocations produced by a bad issuance of the certificate, the holder will be notified in advance to agree on the terms of their replacement.

Camerfirma in any case and under these certification practices, can revoke a certificate unilaterally and immediately for security reasons, without the owner can claim any compensation for this fact.

### 4.9.6 CRL checking requirements

Trusting third parties must first check their use, the status of the certificates, and in any case must verify the last CRL issued, which can be downloaded from the URL that appears in the CRL Distribution Point on each certificate.

Camerfirma always issues CRLs signed by the CA that issued the certificate.

The CRL contains a field (*NextUpdate*) with the date of the next update. However, a new CRL must be issued each time there is a revocation.

### 4.9.7 CRL issuance frequency

| CA | Issuance frequency days | Duration (days) |
|---|---|---|
| CHAMBERS OF COMMERCE ROOT – 2016<br>CHAMBERS OF COMMERCE ROOT – 2018 | Maximum 365 | 365 |
| AC CAMERFIRMA FOR NATURAL PERSONS - 2016 | Immediate - Maximum 1 | 2 |
| AC CAMERFIRMA FOR LEGAL ENTITIES - 2016 | Immediate - Maximum 1 | 2 |
| AC CAMERFIRMA FOR WEBSITES – 2016<br>AC CAMERFIRMA FOR WEBSITES – 2018 | Immediate - Maximum 1 | 2 |
| AC CAMERFIRMA CODESIGN – 2016 | Immediate - Maximum 1 | 2 |
| AC CAMERFIRMA TSA – 2016 | Immediate - Maximum 1 | 2 |
| GLOBAL CHAMBERSIGN ROOT - 2016 | Maximum 365 | 365 |
| AC CAMERFIRMA – 2016 | Maximum 365 | 365 |
| AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016 | Immediate - Maximum 1 | 2 |
| AC CAMERFIRMA GLOBAL FOR LEGAL ENTITIES - 2016 | Immediate - Maximum 1 | 2 |
| AC CAMERFIRMA GLOBAL FOR WEBSITES - 2016 | Immediate - Maximum 1 | 2 |
| AC CAMERFIRMA COLOMBIA – 2016 | Maximum 365 | 365 |
| AC CITISEG – 2016 | Immediate - Maximum 1 | 2 |
| AC CAMERFIRMA PERU – 2016 | Maximum 365 | 365 |
| AC CAMERFIRMA PERU CERTIFICATES – 2016 | Immediate - Maximum 1 | 2 |

### 4.9.8 Maximum latency for CRLs

CRLs are published every 24 hours with a validity of 48 hours.

### 4.9.9 Availability of online service to check revocation

CA provides an online service to check revocations at:

http://www.camerfirma.com/area-de-usuario/consulta-de-certificados/

Also via OCSP queries at:

http://www.camerfirma.com/servicios/respondedor-ocsp/

The addresses to access these services are included in the digital certificate. For the CRLs and ARLs in the CRL Distribution Point extension and the OCSP address in the Authority Information Access extension.

The certificates may include more than one address to access the CRL in order to guarantee availability.

The OCSP service is fed from the CRLs issued by the various certification authorities (CA) or by access to the platform’s database (EE). Technical access data and the OCSP response validation certificates are published on the Camerfirma website http://www.camerfirma.com/servicios/respondedor-ocsp/

*These services are available **24 hours per day, seven days per week, 365 days per year**.*

Camerfirma makes every effort to ensure service is not down for more than **24 hours**. This service is critical for Camerfirma's activities and is therefore considered in the **contingency and business continuity plans**.

### 4.9.10 Requirements of the online service to check revocation

To verify a revocation, the User Party must know the e-mail address related to the certificate that they want to consult if this is accessed online.

**OCSP** responses are signed by the CA that issued the certificate on request; the certificate is required to validate the response. Updated certificates can be found at the link

http://www.camerfirma.com/servicios/respondedor-ocsp/

### 4.9.11 Other methods of disclosing revocation information

Mechanisms that Camerfirma makes available to system users is published on its website http://www.camerfirma.com/area-de-usuario/consulta-de-certificados/

### 4.9.12 Special revocation requirements due to compromised key security

Not stipulated

### 4.9.13 Suspension

*When a certificate suspension takes place, Camerfirma will have* ***one week*** *to decide on the certificate's final status: (revoked or active). If all the information required to verify the status is not provided within this period, Camerfirma will revoke the certificate for unknown reason.*

If the certificate is suspended, a notice is sent to the Subject/Signatory by email specifying the time of suspension and the reason.

If the suspension does not take place and the certificate has to be activated again, the Subject/Signatory will receive an email specifying the new certificate status.

The suspension process does not apply to certificates

- From TSU/TSA
- From CA and Subordinate CA
- From RA Operator.

### 4.9.14 Who can request suspension

See section 4.9.2.

### 4.9.15 Procedure for suspension request

The suspension can be requested by accessing the relevant page on Camerfirma's website or by previously authenticated oral or written communication. The Signatory must have the revocation code in order to suspend the certificate.

### 4.9.16 Suspension period limits

A certificate shall not be suspended for more than **one week**.

Camerfirma supervises, via a certificate management platform alert system (STATUS), that the suspension period established by the Policies and this CPS is not exceeded.

## *4.10 Certificate Status Services*

### 4.10.1 Operational characteristics

Camerfirma provides a service for consulting issued certificates and revocation lists. These services are available to the public on its website: http://www.camerfirma.com/area-de-usuario/consulta-de-certificados/

### 4.10.2 Service availability

Query services are designed to ensure availability 24 hours a day, seven days a week.

### 4.10.3 Optional features

Not stipulated.

## *4.11 End of subscription*

The subscription to the service will end after the validity period of the certificate. As an exception, the subscriber can maintain the current service by requesting the renewal of the certificate, within the advance period determined by this Declaration of Certification Practices.

## *4.12 Key Escrow and Recovery*

### 4.12.1 Key escrow and recovery policy and practices

Camerfirma does not store or copy Signatories' private keys when they are created by the provider. For certificates created on hardware, the user creates and stores the private key on the cryptographic card delivered by the provider.

Camerfirma only stores a copy of the Signatory's private key when it is used "exclusively" for data encryption.

Camerfirma stores Users' keys in PKCS#12 format so that they can be resent in case of download and installation problems. This information is stored for three calendar days only. After this period, the keys are deleted.

### 4.12.2 Session key encapsulation and recovery policy and practices

Not stipulated.

# 5 Physical, Procedural and Personnel Security Controls

## *5.1 Physical Security Controls*

Camerfirma is subject to the annual validations established by the UNE-ISO/IEC 27001 standard, which regulates the establishment of suitable processes to ensure proper security management in information systems.

Camerfirma has established physical and environmental security controls to protect resources in the buildings where the systems and equipment used for the transactions are stored.

The physical and environmental security policy applicable to the certificate creation services provides protection against:

- ✓ Unauthorised physical access
- ✓ Natural disasters
- ✓ Fires
- ✓ Failure in supporting systems (electricity, telecommunications, etc.).
- ✓ Building collapse
- ✓ Flooding
- ✓ Theft
- ✓ Unauthorised withdrawal of equipment, information, devices and applications related to the components used for the Certification Service Provider's services

The facilities have preventive and corrective maintenance services with **24h/365** day per year assistance and assistance during the **24 hours** following the notice.

Reference document: **IN-2005-01-01-Physical access control**

### 5.1.1 Location and building

Camerfirma's facilities are built from materials that guarantee protection against brute force attacks and are located in an area with a low risk of natural disasters and with quick access.

The room where encryption activities take place is a Faraday cage protected against external radiation, with double flooring, fire detection and extinguishing system, damp proof system, dual cooling system and dual power supply system.

Reference document: **IN-2015-01-01-CPD**

### 5.1.2 Physical access

Physical access to Camerfirma's offices where encryption processes are undertaken is limited and protected by a combination of physical and procedural measures.

Access is limited to expressly authorised personnel who must show identification when they access and register, and CCTV cameras film and record any activity.

Any external person must be accompanied by a person in charge of the organisation when they are found within restricted areas for any reason.

The facilities include presence detectors at every vulnerable point as well as intruder alarm systems that send a warning via alternative channels.

The rooms are accessed by ID card scanners which are managed by a software system that maintains an automatic audit log of comings and goings.

The most critical system elements are accessed through three different zones with increasingly limited access.

Access to the certification system is protected by four access levels. Building, offices, DPC and cryptography room.

### 5.1.3 Power supply and air conditioning

Camerfirma’s facilities have voltage stabilisers and a dual power supply system with a generator.

The rooms in which computer equipment is stored have temperature control systems with dual air conditioning units.

### 5.1.4 Exposure to water

Camerfirma’s facilities are in an area with a low flooding risk and are on the first floor. The rooms in which computer equipment is stored have a humidity detection system.

### 5.1.5 Fire protection and prevention

The rooms in which computer equipment is stored have automatic fire detection and extinguishing systems.

Cryptographic devices, and supports that store Certification Entity keys have a specific and additional fire protection system relative to the rest of the facility.

### 5.1.6 Storage systems.

Each demountable storage device (tapes, cartridges, CDs, disks, etc.) is only accessible by authorised personnel.

Regardless of the storage device, confidential information is stored in fireproof or permanently locked cabinets and can only be accessed with express authorisation.

### 5.1.7 Waste disposal

Once sensitive information is no longer useful, it is destroyed using the most appropriate means for the media containing it.

Print-outs and paper: shredders or waste bins are provided for this purpose, for subsequent destruction in a controlled manner.

Storage media: before being thrown away or reused they must be processed for deletion by being physically destroyed, or the contained data made illegible.

Reference document: **IN-2005-01-03-Environmental security**

### 5.1.8 External backup

Camerfirma uses a secure external building to keep documents, magnetic and electronic devices safe, which is separate from the operating centre.

At least two expressly authorised people are required to access, store or withdraw devices.

Related document: **IN-2005-04-06**-Critical file backup procedure

## *5.2 Procedural controls*

### 5.2.1 Roles of trust

Roles of trust are described in the Certification Policies, guaranteeing the distribution of duties to share out control and limit internal fraud and prevent one person from controlling the entire certification process from start to finish, and with minimum privilege granted wherever possible.

To determine the sensitivity of the function, the following items are taken into account:

- Duties associated with the role.
- Access level.
- Monitoring operation.
- Training and awareness.
- Required skills.

**Internal Auditor:**

Responsible for fulfilling the operational procedures. This person does not belong to the Information Systems department.

Internal **Auditor** duties are incompatible with Certification duties and Systems. These duties are subordinated to Operations Management, reporting to this Management and the Technical Department.

**Systems Administrator:**
Responsible for the correct performance of the hardware and software supporting the certification platform.

System administrator tasks are incompatible with certification tasks and cannot perform auditing tasks.

**CA Administrator.**
Responsible for the activities to be undertaken with the cryptographic material or for performing any duties involving the activation of the CA's private keys described herein, or any of its elements.

CA administrator tasks are incompatible with certification and system tasks.

**CA Operator.**
Responsible, together with the CA Administrator, for safekeeping of the cryptographic key activation material, and for CA backup and maintenance procedures.

CA operator tasks are incompatible with CA administrator tasks and cannot perform internal auditor or auditor tasks.

**RA Operator:**
Responsible for approving certification requests from the Signatory.

RA operator operations are incompatible with RA administrator operations nor can they perform internal or external audit tasks.

**Revocation operator:**
Revocation operator tasks are incompatible with audit tasks

**Security Manager:**
To coordinate, monitor and enforce security measures defined by Camerfirma's security policies. Must be responsible for the aspect related to information security: logical, physical, networks, organisational, etc.

IN-2005-02-07 Personnel duties and responsibilities

### 5.2.2 Number of people required per task

Camerfirma guarantees that at least **two people will carry out tasks classified as sensitive**. Mainly handling the Root CA and intermediate CA key storage device.

### 5.2.3 Identification and authentication for each role

The internal auditor assigns the people for each role; this auditor must ensure that each person carries out the procedures to which he/she is assigned.

Each person only controls assets required for his/her role, thereby ensuring that nobody accesses unassigned resources.

Depending on the asset, resources are accessed via cryptographic cards and activation codes.

### 5.2.4 Roles requiring separation of duties

The internal document IN-2016-03-01 job profile file reflects the tasks assigned to the different profiles with a table of segregation of roles.

| | Responsable de Seguridad | Administracion de Sistemas | Oeración de sistemas | Auditor Plataforma CA | Especialidsta Validacion SSL | Operador RA |
|---|---|---|---|---|---|---|
| Responsable de Seguridad | ■ | SI | NO | SI | SI | SI |
| Administracion de Sistemas | NO | ■ | NO | NO | NO | NO |
| Operación de Sistemas | NO | NO | ■ | NO | NO | NO |
| Auditor Plataformas CA | NO | NO | NO | ■ | SI | SI |
| Especialidsta Validacion SSL | NO | NO | NO | SI | ■ | SI |
| Operador RA | NO | NO | NO | NO | SI | ■ |

### 5.2.5 Switching the PKI management system on and off.

The PKI system is formed by the following modules:

**RA Management Module**, for which specific page management services are activated or deactivated.

AC CAMERFIRMA manages two different technical platforms for each hierarchy, although the system is switched off in the same way by deactivating page management services.

**Request management module**, for which specific page management services are activated or deactivated.

**Key management module**, located in the HSM. Activated or deactivated by physically switching it on and off.

**Database module**, centralised certificate management and managed CRLs, OCSP and TSA. Switching the specific database management service on and off.

**OCSP module**. Online certificate status response server. Switching the system service responsible for this task on and off.

**TSA module**. Timestamp server. Switching the service on and off

The module switch-off sequence is:

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

The switching on process is carried out in reverse.

Internal reference document: **IN-2005-05-01**-Manual switching off procedure.

## *5.3 Personnel security controls*

### 5.3.1 Background, qualifications, experience and accreditation requirements

All personnel undertaking tasks classified as duties of trust must have worked at the workplace for at least **one year** and have a fixed employment contract.

All personnel are qualified and have been trained in the procedures to which they have been assigned.

Personnel in positions of trust must have no personal interests that conflict with undertaking the role to which they are entrusted.

Camerfirma ensures that registration personnel or RA Administrators are trustworthy and belong to a Chamber of Commerce or the body delegated to undertake registration work.

RA Administrators must have taken a training course for request validation request duties.

In general, Camerfirma removes an employee’s trust roles if it discovers that person has committed any criminal act that could affect the performance of his/her duties.

Camerfirma shall not assign a trusted or managed site to a person who is not suitable for the position, especially for having been convicted of a crime or misdemeanour affecting their suitability for the position. For this reason, an investigation will first be carried out, to the extent permitted by applicable law, on the following aspects:

- Studies, including alleged degree.

- Previous work, up to five years, including professional references and checking that the alleged work was actually performed.
- Delinquency

Reference documentation:

**IN-2005-02-07-**Personnel duties and responsibilities.

**IN-2005-02-17-**Human Resource Management

**IN-2008-00-06-**Job Profile Format

**IN-2008-00-09-**Training Logs

**IN-2006-02-03-**Security Organisation

### 5.3.2 Background checking procedures

Camerfirma's HR procedures include conducting relevant investigations before hiring anyone.

Camerfirma never assigns duties of trust to personnel who have been working at the company for less than **one year**.

The job application reports on the need to be subjected to undergo prior investigation and warns that refusal to submit to the investigation shall result in the application's rejection. Also, unequivocal consent from the affected party is required for the investigation and for processing and protecting his/her personal data in accordance with the Personal Data Protection law.

### 5.3.3 Training requirements

Personnel undertaking duties of trust must have been trained in accordance with Certification Policies. There is a training plan that is part of the UNE-ISO/IEC 27001 controls.

Registration operators who validate EV secure server certificates receive specific training in accordance with special regulations on issuing these certificates.

Training includes the following content:

- Security principles and mechanisms of the public certification hierarchy.
- Versions of hardware and applications in use.
- Tasks to be carried out by the person.
- Management and processing of incidents and security compromises.
- Business continuity and emergency procedures.
- Management and security procedure related to processing personal data.

### 5.3.4 Information updating requirements and frequency

Camerfirma undertakes the required updating procedures to ensure certification duties are undertaken properly, especially when they are modified substantially.

### 5.3.5 Task rotation frequency and sequence

Not stipulated

### 5.3.6 Penalties for unauthorised actions

Camerfirma has established an internal penalty system, which is described in its HR policy, to be applied when an employee undertakes unauthorised actions, which includes the possibility of dismissal.

### 5.3.7 Personnel hiring requirements

Employees hired to undertake duties of trust must sign the confidentiality clauses and operational requirements that Camerfirma uses. Any action compromising the security of the accepted processes could lead to termination of the employee's contract, once evaluated.

In the event that all or part of the certification services are operated by a third party, the controls and provisions made in this section or in other parts of the CPS are applied and enforced by the third party that performs the operational functions of the certification services, and the certification authority is responsible for the actual implementation in all situations.

These aspects are specified in the legal instrument used to agree on the provision of certification services by third parties other than Camerfirma, and the third parties must be obliged to meet the requirements demanded by Camerfirma.

Reference documentation: **IN-2006-05-02**-Clauses that apply to external developers

### 5.3.8 Documentation given to personnel

Camerfirma provides all personnel with documentation describing the assigned duties, with special emphasis on security regulations and the CPS.

This documentation is in an internal repository accessible by any Camerfirma employee; the repository contains a list of documents of mandatory knowledge and compliance.

Any documentation that employees require is also supplied at any given time so that they can perform their duties competently.

## *5.4 Audit Logging Procedures*

Camerfirma is subject to the annual validations established by the UNE-ISO/IEC 27001 standard, which regulates the establishment of suitable processes to ensure proper security management in information systems.

### 5.4.1 Types of recorded events

Camerfirma records and saves the audit logs of every event relating to the CA’s security system.

The following events are recorded:

- ✓ System switching on and off.
- ✓ Creation, deletion and setting up of passwords or changed privileges.
- ✓ Attempts to log in and out.
- ✓ Attempts at unauthorised access to the CA’s system made online.
- ✓ Attempts at unauthorised access to the file system.
- ✓ Physical access to audit logs.
- ✓ Changes to system settings and maintenance.
- ✓ CA application logs.
- ✓ CA application switching on and off.
- ✓ Changes to the CA’s details and/or passwords.
- ✓ Changes to the creation of certificate policies.
- ✓ Creation of own passwords.
- ✓ Certificate creation and revocation.
- ✓ Logs of destruction of devices containing activation keys and data.
- ✓ Events related to the cryptographic module's lifecycle, such as its reception, use and uninstallation.

Camerfirma also retains the following information, either manually or digitally:

- The key generation event and key management databases.
- Physical access records.
- Maintenance and system configuration changes.
- Personnel changes.
- Reports on compromises and discrepancies.
- Records of the destruction of material containing key information, activation data or personal information about the Signatory for individual certificates or a future key holder for organisation certificates, access to the certificate.
- Possession of activation data for operations with the Certification Authority's private key.
- Complete reports on physical intrusion attempts in infrastructure that support certificate issuance and management.

Camerfirma maintains a system that guarantees:

- Sufficient space for storing audit logs.
- Audit log files are not rewritten.

- That the saved information includes at least the following: event type, date and time, user executing the event and result of the process.
- The audit log files are saved in structured files that can be included in a database for subsequent data mining.

### 5.4.2 Frequency of processing log

Camerfirma checks the audit logs when there is a system alert due to an incident.

Processing audit records involves reviewing records that include verification that they have not been tampered with, a brief inspection of all log entries and further investigation of any alerts or irregularities in the logs. The actions taken from the audit review are documented

### 5.4.3 Retention periods for audit logs

Camerfirma stores the information from audit logs for at least **five years**.

### 5.4.4 Audit log protection

The systems' audit logs are protected against manipulation via signatures in the files that contain them.

They are stored in fireproof devices.

Availability is protected by storing them in buildings outside of the CA's workplace.

Audit log files can only be accessed by authorised persons.

Devices are always handled by authorised personnel.

There is an internal procedure that specifies the procedure to manage devices containing audit log data.

### 5.4.5 Audit Log backup procedures

Camerfirma uses a suitable backup system to ensure that, in the event that important files are lost or destroyed, audit log backups are available for a short period of time.

Camerfirma has implemented a secure backup system for audit logs by making backup copies of every audit log on an external device once per week.

A copy is also kept at an external custody centre.

Reference documentation: **IN-2005-04-10-**audit log management procedure.

### 5.4.6 Audit data collection system

Event audit information is collected internally and automatically by the operating system, the network and by the certificate management software, in addition to the data generated manually, which is stored by duly authorised personnel, all of which makes up the audit record accumulation system.

### 5.4.7 Notifying the party that caused the event

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

It may be communicated whether the result of his/her action was successful or not, but the action is not audited.

### 5.4.8 Vulnerability analysis

The analysis of vulnerabilities is covered by the Camerfirma audit processes. Risk and vulnerability management processes are reviewed once a year in accordance with the UNE-ISO/IEC 27001 certificate and included in the Risk analysis document, code **CONF-2005-05-01**. This document specifies the controls implemented to guarantee required security objectives.

The system audit data is stored so that it can be used to investigate any incident and locate vulnerabilities.

Camerfirma runs a monthly systems analysis with the aim of detecting suspicious activities. This report is executed by an external company and includes:

- Intrusion Detection - IDS (HIDS)
- OSSEC Integrity Control System
- SPLUNK. Operations intelligence.
- Event correlation report.

Camerfirma corrects any problem reported and registered by the systems department.

## *5.5 Records Archival*

### 5.5.1 Type of recorded files.

The following documents that are part of the certificate's life cycle are stored by the CA or RAs:

- ✓ Any system audit data. PKI, TSA and OCSP
- ✓ Any data related to certificates, including contracts with Signatories and the RA. The data relating to their identification and location.
- ✓ Requests to issue and revoke certificates.
- ✓ Type of document submitted in the license application.
- ✓ Identity of the Registration Authority that accepts the certificate application.
- ✓ Unique identification number provided by the previous document.
- ✓ Any issued or published certificates.
- ✓ Issued CRLs or logs of the status of created certificates.
- ✓ Log of created keys.
- ✓ Communications between PKI elements.
- ✓ Certification Policies and Practices

Camerfirma is responsible for correctly filing all this material.

### 5.5.2 File storage period

Certificates, contracts with Subjects/Signatories and any information relating to the Subject/Signatory's identification and authentication must be kept for at least 15 years.

Older versions of documents are also kept for a period of at least fifteen (15) years by AC Camerfirma and may be consulted by stakeholders with reasonable cause.

### 5.5.3 File protection

Camerfirma ensures files are protected by assigning qualified staff to process and store them in fireproof safes in external facilities.

Related document: **IN-2005-04-01-** ***backup management***

### 5.5.4 File backup procedures

Camerfirma has an external storage centre to ensure the availability of digital file backups. The physical documents are stored in secure places restricted to authorised personnel.

Related document: **IN-2005-04-01-** ***backup management***

Camerfirma makes incremental backups of all digital documents at least daily and performs full backups weekly for data recovery purposes.

### 5.5.5 Requirements for log timestamping

Logs are dated with a reliable source via NTP from the ROA, GPS and radio synchronisation systems.

Camerfirma has an IT security document which describes the configuration of the date and time settings for the devices used for certificate issuance.

Related document: **IN-2006-04-01-Time synchronisation**

### 5.5.6 Audit data collection system

Reference documentation: **IN-2005-04-10-**audit log management procedure.

### 5.5.7 Procedures to retrieve and verify filed information

Camerfirma has a software security document that describes the process for checking that the filed information is correct and accessible.

Related document: **IN-2005-04-06**-Critical file backup procedure

## *5.6 Key Changeover*

The **final entity's** keys are changed by starting a new issuance procedure (see the corresponding section of this CPS).

In CA (**Root CA, Subordinate CA**). The key will be changed before the CA certificate expires. The certificate to be updated from the CA and its private key can only be used to sign CRLs while there are active certificates issued by the old CA. A new CA certificate is generated with a new private key and a CN (*common name*) other than the CA certificate to be replaced.

A CA's certificate is also changed when there is a change to cryptographic technology (algorithms, key size, etc.) that so requires it.

Reference document: **IN-2005-04-04-Key changing procedure.**

## *5.7 Compromise and disaster recovery*

If root key security is compromised, this must be considered a specific case in the contingency and business continuity document. If the keys are replaced, this incident affects recognition by the various private and public sector applications. Recovering the validity of keys in business terms mainly depends on the duration of these recognised processes. The contingency and business continuity document include these purely technical and operational terms to ensure that new keys are available, which is not the case for recognition by third parties.

The commitment of algorithms or associated parameters used for generating digital certificates or associated services is also incorporated into the contingency and business continuity plan.

Related Document **IN-2007-02-08 Continuous Improvement Procedure**

### 5.7.1 Incident and compromise handling procedures

Camerfirma has developed a Contingency plan to retrieve critical systems, if an alternative data centre were necessary as part of the UNE-ISO/IEC 27001 certification.

The continuity and contingency plan is drafted in document **CONF-2003-00-01 Continuity and Availability**.

### 5.7.2 Computing resources, software, and/or data are corrupted

Any failure to meet the targets set by this contingency plan is considered reasonably unavoidable unless there is a breach of obligations on Camerfirma's part in implementing these processes.

A part of the implementation of its ISO27001 and ISO20000 systems, Camerfirma has developed plans and procedures for continuous improvement in a way that systematically reinforces all experiences covered in the management of incidents and avoids their repetition.

### 5.7.3 Entity private key compromise procedures

The contingency plan encompassed in Camerfirma's UNE-ISO/IEC 27001 certification considers that compromised security of the CA's private key is a disaster.

If the security of a root key is compromised:

- All Subjects/Signatories, User Parties and other CAs with which agreements or other relationships have been established must be informed.
- They are informed that the certificates and information relating to the revocation status that are signed using this key are not valid.

### 5.7.4 Business continuity capabilities after a disaster

Camerfirma will reinstate critical services (revocation and publication of revocations) in accordance with the contingency and business continuity plan encompassed in the UNE-ISO/IEC 27001 certification, indicating restoration within 24 hours.

Camerfirma has an alternative centre if required to start up the certification systems, which is described in the business continuity plan.

## *5.8 Termination of the CA Activity*

Before Camerfirma ceases its activity, it will:

- Provide the required funds (via a public liability insurance policy) to complete the revocation processes.
- Inform all Subjects/Signatories, User Parties and other CAs with which it has agreements or other types of relationships regarding termination of activity at least **six months** in advance.
- Revoke any authorisation from subcontracted entities to act on behalf of the CA in the certificate issuance procedure.
- Pass on its obligations related to maintaining log data and audit logs for the established time period indicated to Signatories and Users.
- The CA's private keys must be destroyed or disabled.
- Camerfirma will keep any active certificates and the verification and revocation system until all issued certificates have expired.

# 6 Technical Security Controls

## *6.1 Key pair creation and installation*

### 6.1.1 Creating the key pair

The computers used by Camerfirma to store root keys and are certified in accordance with **FIPS 140-2, level 3**.

The root keys are generated and managed on an off-line computer in a cryptographic room. Reference document **CONF-00-2012-02**-Script of CA ROOT generation xxxx where "xxxx" is the year corresponding to the creation of the key.

The creation of Subordinate CAs keys is generated in HSM equipment certified **FIPS 140-2, level 3**, where it is hosted for its corresponding use. The certificate issued by the root key is made in a secure cryptographic room.

| CA | Key length | Signature Algorithm | Creation year | Expiry |
|---|---|---|---|---|
| CHAMBERS OF COMMERCE ROOT - 2016 | 4,096 bits | sha256WithRSAEncryption | 2,016 | 08/04/2040 |
| AC CAMERFIRMA FOR NATURAL PERSONS - 2016 | 4,096 bits | sha256WithRSAEncryption | 2,016 | 09/03/2040 |
| AC CAMERFIRMA FOR LEGAL ENTITIES - 2016 | 4,096 bits | sha256WithRSAEncryption | 2,016 | 09/03/2040 |
| AC CAMERFIRMA FOR WEBSITES - 2016 | 4,096 bits | sha256WithRSAEncryption | 2,016 | 13/03/2040 |
| AC CAMERFIRMA CODESIGN – 2016 | 4,096 bits | sha256WithRSAEncryption | 2,016 | 09/03/2040 |
| AC CAMERFIRMA TSA – 2016 | 4,096 bits | sha256WithRSAEncryption | 2,016 | 09/03/2040 |
| CHAMBERS OF COMMERCE ROOT – 2018 | 4,096 bits | sha256WithRSAEncryption | 2,018 | 10/05/2042 |
| AC CAMERFIRMA FOR WEBSITES - 2018 | 4,096 bits | sha256WithRSAEncryption | 2,018 | 09/04/2042 |
| GLOBAL CHAMBERSIGN ROOT - 2016 | 4,096 bits | sha256WithRSAEncryption | 2,016 | 08/04/2040 |
| AC CAMERFIRMA – 2016 | 4,096 bits | sha256WithRSAEncryption | 2,016 | 09/03/2040 |
| AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016 | 4,096 bits | sha256WithRSAEncryption | 2,016 | 08/02/2040 |
| AC CAMERFIRMA GLOBAL FOR LEGAL ENTITIES - 2016 | 4,096 bits | sha256WithRSAEncryption | 2,016 | 08/02/2040 |
| AC CAMERFIRMA GLOBAL FOR WEBSITES - 2016 | 4,096 bits | sha256WithRSAEncryption | 2,016 | 12/02/2040 |
| AC CAMERFIRMA COLOMBIA – 2016 | 4,096 bits | sha256WithRSAEncryption | 2,016 | 09/03/2040 |
| AC CITISEG – 2016 | 4,096 bits | sha256WithRSAEncryption | 2,016 | 08/02/2040 |
| AC CAMERFIRMA PERU – 2016 | 4,096 bits | sha256WithRSAEncryption | 2,016 | 10/03/2040 |
| AC CAMERFIRMA PERU CERTIFICATES – 2016 | 4,096 bits | sha256WithRSAEncryption | 2,016 | 09/02/2040 |

Further information at http://www.camerfirma.com/area-de-usuario/politicas-y-practicas-de-certificacion/

Reference documentation:

**CONF-00-2012-01** RECORDS from key creation events.

**CONF-00-2012-02/04** Key generation SCRIPTS.
**CONF-00-2012-05** Auditor Report.
**CONF-00-2012-03** Distributing keys among operators.

#### 6.1.1.1 Creating the Signatory's key pair

Subjects/Signatories can create their own keys using Camerfirma-authorised hardware or software devices or Camerfirma can create them in **PKCS#12** software format.

If the certificate is qualified and requires a secure signature creation device it is only used with such devices for digital signatures.

The management platform uses its own resources to generate a random and robust password and a private key protected with this password using the 3DES algorithm. A certificate signing request is generated in PKCS#10 format from that private key. With this request, the CA signs the Signatory's certificate. The certificate is delivered to the user in a PKCS#12 file which includes the certificate and associated private key. The password for the private key and PKCS#12 file is never clear in the system.

Keys are created using the **RSA** public key algorithm.

Keys can also be created in a remote RA system using the web services layer for PKCS#10 request and collection of the corresponding PKCS#7.

The keys have a minimum length of **2048 bits**.

#### 6.1.1.2 Key creation hardware/software

Subjects/Signatories can create their own keys in a Camerfirma-authorised device. See section 6.1.1.1.

The **ROOT** keys use a cryptographic device that complies with **FIPS 140-2 level 3** specifications.

### 6.1.2 Private key delivery to subscriber

See section 3.2.1

### 6.1.3 Delivering the public key to the certificate issuer

The public key is sent to Camerfirma to create the certificate when the circuit so requires. It is sent in standard **PKCS#10** format.

### 6.1.4 Delivering the CA's public key to users

The CA's certificate and fingerprint will be available to users on Camerfirma's web site.

http://www.camerfirma.com/area-de-usuario/descarga-de-claves-publicas/

### 6.1.5 Key Size

The Subject/Signatory's private keys are based on the RSA algorithm with a minimum length of 2048 bits.

The period of use for the public and private key varies depending on the certificate type. See section 6.1.1.

### 6.1.6 Public key creation parameters.

The public key for the Root CA and Subordinate CA and for Signatories' certificates is encrypted pursuant to RFC 3280 and PKCS#1. RSA is the key generation algorithm.

- Key size = minimum 2,048 bits
- Key creation algorithm: rsagen1
- Padding scheme: emsa-pkcs1-v1_5
- Hash functions: SHA-256

### 6.1.7 Key usage purposes

All certificates issued contain the "KEY USAGE" and "EXTENDED KEY USAGE" attributes, as defined by the X.509v3 standard. More information is available in section 7.1.2.

## *6.2 Private Key Protection and Cryptographic Module Engineering Controls*

### 6.2.1 Cryptographic module standards and controls

#### 6.2.1.1 The Signatory's private key

The Signatory's private key can be stored in a software or hardware device.

When it is stored in software format, Camerfirma provides configuration instructions for secure use.

Cryptographic devices distributed by Camerfirma to host qualified certificates must meet all requirements of qualified secure signature creation devices and therefore are suitable for generating qualified signatures.

Information regarding the key creation and custody process that Camerfirma uses is included in the digital certificate itself, in the corresponding OID, allowing the User Party to act in consequence.

**Reference documentation:**

**CONF-2016-04-02-**Protecting and Activating Online CA Keys

**CONF-2012-04-10** - Certificate issue ceremony script.

#### 6.2.1.2 The CA's private key

The private signature key of the root CAs and Subordinate CAs are maintained in a cryptographic device that meets **FIPS 140-2 level 3** specifications.

When the CA's private key is outside the device, it is kept encrypted.

A backup is made of the CA private key which is stored and only retrieved by authorised personnel in accordance with the roles of trust, using at least dual control on a secure physical device.

The CA's private key backups are stored securely. This procedure is described in detail in the Camerfirma security policies.

Subordinate CAs' keys are kept on devices that comply with at least **FIPS 140-1 Level 3**.

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

Multi-person control is required for activation of the CA's private key. In accordance with this CPS, there is a policy of **two of four people** in order to activate keys.

Reference documentation: **CONF-00-2012-03-Distributing keys among operators**

### 6.2.3 Private key escrow

Camerfirma does not store or copy the private keys of the owners. Only in case of certificates for information encryption Camefirma saves a copy of said key.

### 6.2.4 Private key backup

Camerfirma makes backups of CA private keys to allow their retrieval in the event of natural disaster, loss or damage. At least two people are required to create the copy and retrieve it.

These retrieval files are stored in fireproof cabinets and in an external custody centre.

The Signatory's keys created on software can be stored for retrieval in the event of a contingency in an external storage device separately from the installation key, as specified in the software key installation manual.

The Signatory's keys created on hardware cannot be copied because they cannot be taken out of the cryptographic device.

Camerfirma keeps records on CA private key management processes.

Reference documentation: **CONF-00-2012-01-Minutes on backup of root CA keys.**

### 6.2.5 Archiving the private key

The CAs private keys are filed for at least **10 years** after the last certificate has been issued. They are stored in secure fireproof cabinets in the external custody centre. At least two people are required to retrieve the CA's private key from the initial cryptographic device.

Signatories may store keys delivered on software for the certificate duration period, but must then destroy them and ensure they have no information encrypted with the public key.

Signatories can only store the private key for as long as they deem appropriate in the case of encryption certificates. In this case, Camerfirma will also keep a copy of the private key associated with the encryption certificate.

When PKCS#12 format is used, Camerfirma ensure the elimination of user keys by executing a daily task. This task verifies that three business days have not passed from the date of generation of the certificate. The folder where the files are stored has a filter that prevents files with extension p12 being backed up.

Camerfirma keeps records on CA private key management processes.

### 6.2.6 Entering the private key in the cryptographic module.

CA keys are created inside cryptographic devices. See Camerfirma CA key creation events.

CONF-00-2012-01/06/07/08 RECORDS from key creation events.

Keys created on the Signatories' software are created in Camerfirma's systems and are delivered to the end Signatory in a PKCS#12 software device. See Signatory key creation procedure.

Keys created on Signatories' hardware are created inside the cryptographic device delivered by the CA. See Signatory key creation procedure.

At least two people are required to enter the key in the cryptographic module.

Keys associated with Signatories cannot be transferred.

Camerfirma keeps records on CA private key management processes.

### 6.2.7 Private key storage on cryptographic module

The CA ROOT keys are kept stored in the PCI cryptographic module with the associated equipment disconnected when no operation is being performed.

The keys of the intermediate CAs are stored in HSM network equipment online, so that they can be accessed from the PKI applications for the generation of certificates.

### 6.2.8 Private key activation method.

The Signatory's private key is accessed via an activation key, which only the Signatory knows and must avoid writing down.

The CA Root's key is activated via an m out of n process. See section 6.3.1

Intermediate CA private key activation is managed by the management application.

Reference documentation: **CONF-2008-04-09-Acceso_PKCS#11_CAS_online**

Camerfirma keeps records on CA private key management processes.

### 6.2.9 Private key deactivation method

For certificates on a card, the Signatory's private key is deactivated once the cryptographic device used to create the signature is removed from the reader.

When the key is stored in software, it can be deactivated by deleting the keys from the application in which they are installed.

The CA's private keys are deactivated following the steps described in the cryptographic device administrator's manual.

For Root, CA, Subordinate CA and TSU entity keys, there is a cryptographic event from which the corresponding record is made.

### 6.2.10 Private key destruction method

Before the keys are destroyed, a revocation of the certificate of the public key associated with them is issued.

Devices that have any part of the private keys belonging to the Hierarchy CAs are destroyed or restarted at a low level. The steps described in the cryptographic device administrator's manual are followed to eliminate them.

Backups are destroyed securely.

The Signatory's keys stored on software can be destroyed by deleting them in accordance with instructions from the application on which they are stored.

The Signatory's keys on hardware can be destroyed using special software at the Registration points or the CA's facilities.

Camerfirma keeps records on CA private key management processes.

### 6.2.11 Cryptographic Module Rating

Cryptographic modules are certified FIPS-140-2 level 3 are managed by at least two operators in a model n of m. The teams are housed in secure environments. The cryptographic module that stores the Root keys is managed inside an isolated and disconnected cryptographic room. The cryptographic modules that store the SubCA keys are stored in secure environments within a CPD following ISO27001 regulations.

## *6.3 Other aspects of managing key pairs*

### 6.3.1 Archiving the public key

The CA maintains its archives for a minimum period of **fifteen (15) years** provided that the technology at the time allows this. The documentation to be kept includes public key certificates issued to Signatories and proprietary public key certificates.

### 6.3.2 Period of use for public and private keys

The private key must not be used once the validity period of the associated public key certificate has expired.

The public key or its public key certificate can be used as a mechanism for verifying encrypted data with the public key outside the temporary scope for validation work.

A private key can only be used outside the period established by the digital certificate to retrieve the encrypted data.

## *6.4 Private key activation data.*

### 6.4.1 Generation.

The activation data of the user's private key is generated differently depending on the type of certificate.

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

**On the Camerfirma hardware device.** Cards used by Camerfirma are generated protected with a factory-calculated PIN and PUK. This information is sent by the management platform to the Subject via the email address associated with the digital certificate. The Subject has software to change their card's PIN and PUK.

**On a third party hardware device.** AC Camerfirma accredits third-party devices, even though they are managed separately.

### 6.4.2 Activation data protection

Activation data is communicated to the Subject by an independent channel. AC Camerfirma stores this information in its database. Data can be sent back to the subject at prior request to the email address associated with the certificate, and it is effective as long as the user has not previously changed it.

### 6.4.3 Other activation data aspects

Not stipulated.

## *6.5 Computer security controls*

Camerfirma uses reliable systems to provide certification services. Camerfirma has undertaken IT controls and audits to manage its IT assets with the security level required for managing digital certification systems.

In relation to information security, the certification model on ISO 270001 information management systems is followed.

Computers used are initially configured with the appropriate security profiles by Camerfirma system personnel, for the following aspects:

1. Operating system security settings.
2. Application security settings.
3. Correct system dimensioning.
4. User and permission settings.
5. Configuring audit log events.
6. Back-up and recovery plan.
7. Antivirus settings
8. Network traffic requirements

### 6.5.1 Specific computer security technical requirements

Each Camerfirma server includes the following functions:

- ✓ access control to CA services and privilege management.
- ✓ separation of tasks for managing privileges
- ✓ identification and authentication of roles related to identities

- ✓ the Signatory's and CA's log file and audit data
- ✓ audit of security events
- ✓ self-diagnosis of security related to CA services
- ✓ Key and CA system retrieval mechanisms

The functions described above are carried out using a combination of operating system, KPI software, physical protection and procedures.

### 6.5.2 Computer security appraisal

Computer security is shown in an initial risk analysis, such that the security measures applied are a response to the probability of a group of threats breaching security and their impact.

## *6.6 Lifecycle security controls*

The certificates store the Signatory's keys in a qualified signature creation device **(Hardware)**.

The hardware device is a cryptographic card or USB token certified as a qualified signature creation device in compliance with Appendix II of e-IDAS.

As regards hardware devices

a) Hardware devices are prepared and sealed by an external provider.
b) The external provider sends the device to the registration authorities to be delivered to the Signatory.
c) The Signatory or RA uses the device to generate the key pair and send the public key to the CA.
d) The CA sends a public key certificate to the Signatory or RA, which is entered into the device.
e) The device can be reused and can store several key pairs securely.
f) The device is owned by the Subject/Signatory.

### 6.6.1 System development controls

Camerfirma has established a procedure to control changes to operating system and application versions that involve upgrades to security functions or to resolve any detected vulnerability.

In response to intrusion and vulnerability analyses, adaptations are made to systems and applications that may have security problems, and to security alerts received from managed security services contracted with third parties. The corresponding RFCs (Request for

Changes) are sent so that security patches can be incorporated or the versions with problems updated.

The RFC is incorporated and the measures taken for acceptance, implementation or rejection of the change are documented.

In cases where the implementation of the update or correction of a problem entails a situation of vulnerability or a significant risk, it is included in the risk analysis and alternative controls are implemented until the risk level is acceptable.

Reference documentation:

**IN-2006-05-02-Clauses that apply to external developers**

**IN-2006-03-04-Systems and Software Change Control**

## 6.6.2 Security management controls

### 6.6.2.1 Security management

Camerfirma organises the required training and awareness activities for employees in the field of security. The training materials used and the process descriptions are updated once approved by a security management group.

An annual training plan has been established for such purposes.

Camerfirma establishes the equivalent security measures for any external provider involved in certification work in contracts.

### 6.6.2.2 Data and asset classification and management

Camerfirma maintains an inventory of assets and documentation and a procedure to manage this material to guarantee its use.

Reference documentation: **IN-2005-02-15**-Asset Classification and Inventory

Camerfirma's security policy describes the information management procedures, classifying them according to level of confidentiality.

Documents are classified into three levels: PUBLIC, INTERNAL USE AND CONFIDENTIAL.

Reference documentation: **IN-2005-02-04-Security Policy**

### 6.6.2.3 Management procedures

Camerfirma has established an incident management and response procedure via an alert and periodic reporting system. Camerfirma's security document describes the incident management process in detail.

Reference documentation: **IN-2010-10-08 Incident management**

Camerfirma records the entire procedure relating to the functions and responsibilities of the personnel involved in controlling and handling elements of the certification process.

Reference documentation: **IN-2005-02-07 Personnel duties and responsibilities**

### Processing devices and security

All devices are processed securely in accordance with information classification requirements. Devices containing sensitive data are destroyed securely if they are no longer required.

Camerfirma has a systems fortification procedure in which the processes for secure installation of equipment are defined. The measures described include disabling services and accesses not used by the installed services.

Reference documentation:

**CONF-2006-01-04-Device Input and Output Registration Procedure**
**IN-2012-04-03-Security Operating Procedures for System Fortification.**

### System planning

Camerfirma's Systems department maintains a log of equipment capacity. Together with the resource control application, each system can be re-dimensioned.

Related documentation:

**IN-2010-10-10 Configuration management**

**IN-2010-10-05 Capacity Management**

**IN-2010-10-03 Availability Management**

**IN-2010-10-01 Service Level Management**

**IN-2010-10-00 IT Services Management Manual**

**IN-2010-10-13 New Services Planning**

### Incident reporting and response

Camerfirma has established a procedure to monitor incidents and resolve them, including recording of the responses and an economic evaluation of the incident solution.

Reference documentation: **IN-2010-10-08 Incident management**

### Operating procedures and responsibilities

Camerfirma defines activities, assigned to people with a role of trust other than the people responsible for carrying out daily activities that are not confidential.

Reference documentation: IN-2005-02-07 Personnel duties and responsibilities

### 6.6.2.4 Access system management

Camerfirma makes every effort to ensure access is limited to authorised personnel.

Reference documentation: **IN-2011-04-10 Network access control**.

In particular:

### General CA

a) There are controls based on firewalls, antivirus and IDS with high availability.

b) Sensitive data is protected via cryptographic methods or strict identification access controls.

c) Camerfirma has established a documented procedure to process user registrations and cancellations and a detailed access policy in its security policy.

d) Camerfirma has implemented procedures to ensure tasks are undertaken in accordance with the roles policy.

e) Each person is assigned a role to carry out certification procedures.

f) Camerfirma employees are responsible for their actions in accordance with the confidentiality agreement signed with the company.

### Creating the certificate

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

### Revocation management

Revocation takes place via strict card-based authentication of an authorised administrator's applications. The audit log systems generate evidence that guarantees non-repudiation of the action taken by the CA administrator.

### Revocation status

The revocation status application includes access control based on authentication via certificates to prevent attempts to change the revocation status information.

#### 6.6.2.5 Managing the cryptographic hardware lifecycle

Camerfirma inspects the delivered material to make sure that the cryptographic hardware used to sign certificates is not manipulated during transport.

Cryptographic hardware is transported using means designed to prevent any manipulation. Camerfirma records all important information contained in the device to add to the assets catalogue.

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

Camerfirma runs regular tests to ensure the device is in perfect working order.

The cryptographic hardware device is only handled by trustworthy personnel.

The CA's private signature key stored in the cryptographic hardware will be deleted once the device has been removed.

The CA's system settings and any modifications and updates are recorded and controlled.

Camerfirma has established a device maintenance contract. Any changes or updates are authorised by the security manager and recorded in the corresponding work records. These configurations are carried out by at least two trustworthy employees.

### 6.6.3 Lifecycle security evaluation

Not stipulated

## *6.7 Network security controls*

Camerfirma protects physical access to network management devices and has an architecture that sorts traffic based on its security characteristics, creating clearly-defined network sections. These sections are divided by firewalls.

Confidential information transferred via insecure networks is encrypted using SSL protocols.

The policy used to configure security systems and elements is to start from an initial state of total blocking and to open the services and ports necessary for executing the services. Reviewing accesses is one of the tasks carried out in the systems department.

Management systems and production systems are in separate environments as indicated in the reference document.

Reference documentation: **IN-2011-04-10 Network access control**.

## *6.8 Time Sources*

Camerfirma has established a time synchronisation procedure in coordination with the ROA Real Instituto y Observatorio de la Armada (Royal Navy Institute) in San Fernando via NTP. It also obtains a secure source via GPS and radio synchronisation. Reference documentation: **IN-2006-04-01-Time synchronisation**

# 7 Certificate Profiles and CRL

## *7.1 Certificate Profile*

Certificate profiles comply with RFC 5280.

All qualified or recognised certificates issued in accordance with this policy comply with standard X.509 version 3, and RFC 3739 and the different profiles described in the EN 319 412 standard.

The profile records for these certificates can be requested from gestion_soporte@camerfirma.com or by telephone 902 361 207

### 7.1.1 Version number

Camerfirma issues X.509 certificates Version 3

### 7.1.2 Certificate extensions

Certificate extension documents are described in the profile files. The profile records can be requested from gestion_soporte@camerfirma.com or by telephone 902 361 207

### 7.1.3 Algorithm object identifiers (OID)

The signature algorithm object identifier would be:

- 1.2.840.113549.1.1.11 - sha256WithRSAEncryption
- 1.2.840.113549.1.1.13 – sha512WithRSAEncryption

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

### 7.1.4 Name format.

Certificates must contain the information that is required for its use, as determined by the corresponding authentication policy, digital signature, encryption or digital evidence.

In general, certificates for use in the public sector must contain the identity of the person who receives them, preferably in the Subject Name or Subject Alternative Name fields, including the following data:

- The full name of the Signatory person, certificate holder or represented, in separate fields, or indicating the algorithm that allows the separation automatically.
- Name of the legal entity, where applicable.

- Numbers of the corresponding identification documents, in accordance with the law applicable to the Signatory person, certificate holder or represented, whether a natural person or a legal entity.

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

The exact semantics of the names described in the profile files. The profile records can be requested from gestion_soporte@camerfirma.com or by telephone 902 361 207

### 7.1.5 Name restrictions

Camerfirma may use name restrictions (using the "name constraints" certificate extension) in Subordinate CA certificates issued to third parties so that only the set of certificates allowed in this extension can be issued by the Subordinate CA.

### 7.1.6 Certification Policy (OID) object identifier

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

### 1.1.1 Using the "Policy Constraints" extension

Camerfirma may use policy restrictions (using the "*policy constraints*" certificate extension) in Subordinate CA certificates issued to third parties so that only the set of certificates allowed in this extension can be issued by the Subordinate CA.

### 7.1.7 Syntax and semantics of policy qualifiers

Not stipulated

### 7.1.8 Semantic treatment for the critical extension "Certificate Policy"

The "Certificate Policy" extension identifies the policy that defines the practices that Camerfirma explicitly associates with the certificate. The extension may contain a qualifier from the policy. See 7.1.6.

## *7.2 CRL Profile*

The CRL profile matches the one proposed in the relevant certification policies. The CRLs are signed by the CA that issued the certificates.

The CRL's detailed profile can be requested from gestion_soporte@camerfirma.com or by telephone 902 361 207.

### 7.2.1 Version number

The CRLs issued by Camerfirma are version 2.

### 7.2.2 CRL and extensions

Those established in the certification policies. The detailed profile of the CRL and its extensions can be requested from gestion_soporte@camerfirma.com or by telephone 902 361 207.

## *7.3 OCSP Profile*

### 7.3.1 Version number

The OCSP Responder certificates are Version 3. These certificates are issued by each CA managed by AC Camerfirma according to the RFC 6960 standard.

### 7.3.2 OCSP Extensions

The profile of the OCSP responder certificates can be obtained from gestion_soporte@camerfirma.com or by telephone 902 361 207.

An updated list of OCSP certificates can be obtained from http://www.camerfirma.com/servicios/respondedor-ocsp list.

# 8 Compliance Audit and Other Assessment

Camerfirma is committed to the security and quality of its services.

Camerfirma's objectives in relation to security and quality have essentially involved obtaining ISO/IEC 27001, ISO/IEC 20000 certification and carrying out biennial audits on its certification system, and essentially on the Registration Authorities, in order to guarantee compliance with internal procedures.

Camerfirma is subject to regular audits, with the ***WEBTRUST for CA***, ***WEBTRUST SSL BR*** and ***WEBTRUST EV*** seal, which guarantees that the policy and CPS documents have the appropriate format and scope and are fully aligned with their certification policy and practices.

In order to comply with eIDAS requirements, AC Camerfirma undertakes a biennial compliance evaluation as established in the regulation of the following standards: **EN 319 401, EN 319 411-1, EN 319 411-2, EN 319 421.**

The **Registration Authorities** belonging to both hierarchies are subject to an internal audit process. These audits are conducted periodically on a discretionary basis based on a risk assessment by the number of certificates issued and number of registration operators, which also determines whether the audit is carried out on site or remotely. The audits are described in an "Annual Audit Plan".

AC Camerfirma is subject to a biennial Spanish Personal Data Protection Act audit.

AC Camerfirma performs an internal audit on entities that have obtained a **Subordinate CA** or **TSU** certificate and that issue and manage certificates with their own technical and operational resources. In this audit, Camerfirma randomly checks a number of certificates issued by this registration authority, ensuring that the evidence collected is correct and sufficient for the issuance of the certificate.

## *8.1 Audit frequency*

Camerfirma conducts an annual compliance audit, in addition to the internal audits performed on a discretionary basis.

- **ISO 27001** and **ISO20000** auditing on a three-year cycle with annual reviews.
- **WEBTRUST for CA, WEBTRUST SSL BR, WEBTRUST EV SSL** annually.
- **eIDAS** Conformity Assessment, biennial with annual review
- **Spanish Personal Data Protection Act** audit, biennial with annual review.
- **RA** audits on a discretionary basis.
- **Internal** Audits, External Subordinate CAs, External TSUs, on a discretionary basis.

### 8.1.1 External Subordinate CA audits.

Through its auditors, AC Camerfirma conducts an annual audit on the organisations that have obtained a Subordinate CA or TSA certificate and that issue certificates with their own technical and operational resources. This audit can be replaced by a favourable ***WebTrust for CA*** and/or ***WebTrust for EV*** audit certificate as applicable to the certificates issued.

### 8.1.2 Auditing the Registration Authorities

Every RA is audited. These audits are performed at least every two years on a discretionary basis and based on a risk analysis. The audits check compliance with the Certification Policy requirements in relation to undertaking the registration duties established in the signed service agreement.

As part of the internal audit, samples are taken of the certificates issued to check they have been processed correctly.

Reference documentation regarding the RA audit process are:

**IN-2010-04-12**-RA Security Evaluation Procedure
**IN-2010-04-15**-Ficha de la visita de evaluación.doc
**IN-2010-04-16**-Check List
**IN-2006-03-08**-RA Work Procedures.
**IN-2010-04-17**-Evaluation Report

## *8.2 Auditor identification and rating*

The audits are conducted by independent external companies that are widely renowned in computer security, information systems security and in compliance audits by Certification Authorities:

- For the WEBTRUST - AUREN audit:http://www.auren.com.
- For ISO27001/20000 AENOR audits. http://www.aenor.es/aenor/inicio/home/home.asp
- For internal audits / RA / Subordinate CA, TSA Spanish Personal Data Protection Act – AUREN http://www.auren.com/
- For conformity assessment of eIDAS Natural Person & Legal Person. – TÜVIT https://www.tuvit.de/en/
- For eIDAS conformity assessment of CSQA Timestamps and Certificates Website https://www.csqa.it/

## *8.3 Relationship between the auditor and the CA*

The audit companies used are independent and reputed companies with specialist IT audit departments that manage digital certificates and trusted services, which rules out any conflict of interest that may affect their activities in relation to the CA.

There is no financial or organisational association between auditing firms and AC Camerfirma.

## *8.4 Topics covered in the audit*

In general terms, the audits verify:

a) That Camerfirma has a system that guarantees service quality.
b) That Camerfirma complies with the requirements of the Certification Policies that regulate the issuing of the different digital certificates.
c) That the CPS is in keeping with the provisions of the Policies, with that agreed by the Authority that approves the Policy and as established under current law.
d) That Camerfirma properly manages the security of its information systems.
e) In the OV and EV certificates, the audit checks variance with the policies established by CABFORUM in the "*Baseline Requirements*" as well as "*EV SSL Certificate guidelines*".

In general, the elements audited are:

- Camerfirma processes, RAs and related elements in the issuing of TSA timestamp certificates and validation of services in OCSP line.
- Information systems.
- Protecting the data processing centre.
- Documentation required for each type of certificate.
- Verification that the RA operators know AC Camerfirma's CPS and Policies

## *8.5 Processing the audit report*

Once the compliance report from the audit is received, Camerfirma discusses any deficiencies found with the entity that carried out the audit and develops and implements a corrective plan in order to address the shortcomings.

If the audited entity is unable to develop and/or implement the plan within the time frame requested, or if the deficiencies pose an immediate threat to the system's security or integrity, the policy authority must be notified immediately, and may take the following actions:

- Cease operations temporarily.
- Revoke the corresponding certificate, and restore infrastructure.
- Terminate service to the Entity.
- Other complementary actions as may be needed.

## *8.6 Communication of results*

The communication of results will be carried out by the auditors who have carried out the evaluation to the person in charge of security and regulatory compliance. It is carried out in an act with the presence of the corporate management. The audit certificate is published on the Camerfirma website.

# 9 Administration specification.

## *9.1 Fees*

### 9.1.1 Price for certificate issuing and renewal.

The prices for certification services or any other related services are available and updated on Camerfirma's website

http://www.camerfirma.com/certificados/ or by prior consultation with the Camerfirma support department athttps://secure.camerfirma.com/incidencias/ or by telephone 902 361 207.

The specific price is published for each type of certificate, except those subject to previous negotiation.

### 9.1.2 Prices for access to certificates.

Access to certificates is free-of-charge, although AC Camerfirma applies controls in order to avoid mass certificate downloads. Any other situation that Camerfirma deems must be considered in this respect will be published on Camerfirma's websitehttp://www.camerfirma.com/certificados/ or by prior consultation with the Camerfirma support department at https://secure.camerfirma.com/incidencias/ or by telephone: 902 361 207.

### 9.1.3 Prices for access to information relating to the status of certificates or renewed certificates.

Camerfirma provides free access to information relating to the status of certificates or revoked certificates via certificate revocation lists or via its website http://www.camerfirma.com/area-de-usuario/consulta-de-certificados/.

Camerfirma offers the OCSP service free-of-charge
http://www.camerfirma.com/servicios/respondedor-ocsp/.

### 9.1.4 Prices for access to the contents of these certification practices.

Access to the content of this CPS is free-of-charge on Camerfirma's website https://policy.camerfirma.com.

### 9.1.5 Refund policy.

AC Camerfirma does not have a specific refund policy, and adheres to general current regulations.

## *9.2 Financial Responsibility*

### 9.2.1 Insurance coverage

Camerfirma, in its role as a CSP, has a public liability insurance policy that covers its liabilities to pay compensation for damages and losses caused to the users of its services: the Subject/Signatory and the User Party and third parties, for a total amount of **3,700,000 euros**.

### 9.2.2 Other assets

Not stipulated

### 9.2.3 Insurance or warranty coverage for end-entities

See section 9.2.1

## *9.3 Confidentiality*

### 9.3.1 Type of information to be kept confidential

Camerfirma considers any information not classified as public to be confidential. Information declared confidential is not disclosed without express written consent from the entity or organisation that classified this information as confidential, unless established by law.

Camerfirma has established a policy for processing confidentiality agreement information and forms, which anyone accessing confidential information must sign.

Reference documentation:

**IN-2005-02-04**-Security Policy.
**IN-2006-02-03**-Security Regulations.

### 9.3.2 Type of information considered not confidential

Camerfirma considers the following information not confidential:

a) The contents of this CPS and the Certification Policies
b) The information contained in the certificates.
c) Any information whose accessibility is prohibited by current law.

### 9.3.3 Disclosure of information about certificate revocation/suspension

Camerfirma discloses information on the suspension or revocation of a certificate by periodically publishing corresponding CRLs.

Camerfirma provides a CRL and Certificate query service on the following website: http://www.camerfirma.com/area-de-usuario/consulta-de-certificados/

Camerfirma has an online query service for the status of certificates based on the OCSP standard at http://ocsp.camerfirma.com. The OCSP service provides standardised responses about the status of a digital certificate under the RFC 2560; in other words, whether the certificate consulted is active, revoked or whether it has been issued by the certification authority.

The policy for dissemination of information about certificate revocation in External Subordinate CAs with use of proprietary technology is based on their own CPS.

### 9.3.4 Sending information to the Competent Authority

Camerfirma will provide the information that the competent authority or corresponding regulatory entity requests in compliance with current law.

## *9.4 Privacy of Personal Information*

### 9.4.1 Privacy plan

Camerfirma complies strictly with current data protection law. In this sense, in accordance with Law 59/2003 on Digital Signatures (Article 19.3), this document serves as a security document.

Reference documentation:

**IN-2006-05-11**-Compliance with legal requirements

### 9.4.2 Information treated as private

Personal information about an individual that is not publicly available in the contents of a certificate or CRL is considered private.

### 9.4.3 Information not considered private

The personal information about an individual available in the contents of a certificate or CRL, is considered as non-private when it is necessary to provide the contracted service, without prejudice to the rights corresponding to the holder of the personal data under the LOPD / legislation. RGPD.

### 9.4.4 Responsibility to protect private information

It is the responsibility of the controller to adequately protect private information.

### 9.4.5 Notice and consent to use private information

Before entering into a contractual relationship, Camerfirma will offer interested parties prior information about the processing of their personal data and the exercise of rights, and, if applicable, will obtain the mandatory consent for the differentiated treatment of the main treatment for the provision of contracted services.

### 9.4.6 Disclosure in accordance with a judicial or administrative process

Personal data that are considered private or not, may only be disclosed if necessary for the formulation, exercise or defense of claims, either by a judicial procedure or an administrative or extrajudicial procedure.

### 9.4.7 Other circumstances of disclosure of information

Personal data will not be transferred to third parties except legal obligation.

## *9.5 Intellectual Property Rights*

Camerfirma owns the intellectual property rights on this CPS. The CPS of Subordinate CAs associated with Camerfirma hierarchies is owned by Camerfirma, without prejudice to the assignments of use of their rights in favour of Subordinate CAs and without prejudice to the contributions of the Subordinate CAs that are owned by them.

## *9.6 Representations and Warranties*

### 9.6.1 CA representations and warranties

#### 9.6.1.1 CA

In accordance with the stipulations of the Certification Policies and this CPS, and in accordance with current law regarding certification service provision, Camerfirma undertakes to:

- Adhere to the provisions within the scope of this CPS and the corresponding Certification Policies.
- Protect its private keys and keep them secure.
- Issue certificates in accordance with this CPS, the Certification Policies and the applicable technical standards.
- Issue certificates in accordance with the information in its possession and which do not contain errors.
- Issue certificates with the minimum content defined by current law for qualified or recognised certificates.
- Publish issued certificates in a directory, respecting all legal provisions regarding data protection.
- Suspend and revoke certificates in accordance with this Policy and publish the revocations in the CRL.
- Inform Subjects/Signatories about the revocation or suspension of their certificates, on time and in accordance with current law.
- Publish this CPS and the Certification Policies on its website.
- Report changes to this CPS and the Certification Policies to the Subjects/Signatories and its associated RAs.
- Do not store or copy the Subject/Signatory's signature creation data except for encryption certificates and when it is legally provided for or allowed to be stored or copied.
- Protect data used to create the signature while in its safekeeping, if applicable.
- Establish data creation and custody systems in the aforementioned activities, protecting data from being lost, destroyed or forged.
- Keep data relating to the issued certificate for the minimum period required by current law.

Camerfirma's responsibility

Article 22.1 of the Law on Digital Signatures establishes that:

> "Certification service providers are responsible for damages and losses caused to any person during their activities in the event they breach the obligations established in this Law.
>
> The certification service provider regulated herein shall be held liable in accordance with general regulations on contractual or non-contractual liability, as applicable,

> although the certification service provider must prove that it acted with due professional diligence.”

Article 13 of the eIDAS regulation provides:

> *1. Without prejudice to the provisions of paragraph 2, trusted service providers are responsible for damages caused intentionally or negligently to any natural person or legal entity for breach of its obligations under this Regulation.*
>
> *The burden of proof of intent or negligence of an unqualified trusted service provider corresponds to the natural person or legal entity claiming the damages that the first paragraph refers to.*
>
> *The intent or negligence of a qualified trusted service provider is presumed unless the qualified trusted service provider proves that the damage referred to in the first paragraph occurred without intent or negligence on its part.*
>
> *2. When a service provider duly informs its customers in advance about the limitations of the use of the services provided and these limitations are recognisable to a third party, the trusted service provider is not responsible for damages caused by use of services beyond the limitations stated.*
>
> *3. Paragraphs 1 and 2 shall apply in accordance with Spanish liability regulations.*

Camerfirma is responsible for any damages or losses caused to users of its services, whether the Subject/Signatory or the User Party, and other third parties in accordance with the terms and conditions established under current law and in the Certification Policies.

In this sense, Camerfirma is the only party responsible for (i) issuing the certificates, (ii) managing them throughout their lifecycle and (iii) in particular, if necessary, in the event of suspension and revocation of the certificates. Specifically, Camerfirma is fundamentally responsible for:

- The accuracy of the information contained in the certificate on the date of issue by confirming the applicant’s details and the RA practices.
- Guaranteeing that when the certificate is delivered, the Subject/Signatory is in possession of the private key relating to the public key given or identified in the certificate when required, by using standard request forms in PKCS#10 format.
- Guaranteeing that the public and private keys work in conjunction with each other, using certified cryptographic devices and mechanisms.
- That the certificate requested and the certificate delivered match.
- Any liability established under current law.

In accordance with current law, Camerfirma holds a public liability insurance policy that fulfils the requirements established in the certification policies affected by these certification practices.

#### 9.6.1.2 External Subordinate CA.

External Subordinate CAs are CAs incorporated into the root CA's hierarchy but are owned by a different organisation and may or may not use a different technique or infrastructure.

- Protect their private keys.
- Issue certificates pursuant to certification policies and/or corresponding CPS.
- Issue certificates that are free from errors.
- Publish issued certificates in a directory, respecting all legal provisions regarding data protection.
- Allow an annual audit by AC Camerfirma.
- Safeguard, for the duration established by law, the documentary information and systems that have been used or generated for issuing certificates.
- Notify AC Camerfirma of any incident in the delegated activity.

Responsibility of the Subordinate CA (Internal/External).

Without prejudice to Camerfirma's responsibility for issuing and revoking digital certificates of Subordinate CAs as well as the agreed contractual terms in each case, the Subordinate CAs (through the legal entity on which they depend) are responsible for issuing and revoking digital certificates issued to the end user, responding to the Signatories and other third parties or users affected by the service in accordance with their own Certification Practices Statements, Certification Policies and national legislation, if applicable.

### 9.6.2 RA representations and warranties

RAs are entities that the CA appoints to register and approve certificates; therefore, the RAs also carry out the obligations defined in the Certification Practices for issuing certificates, particularly to:

- Adhere to the provisions of this CPS and the Certification Policy.
- Protect their private keys that are used for exercising their functions.
- Check the identity of the Subjects/Signatories and Applicants of certificates when necessary, definitively proving the Signatory's identity, for individual certificates, or the key holder, for organisation certificates, pursuant to the provisions of the corresponding sections of this document.
- Check the accuracy and authenticity of information provided by the Applicant.

- Provide the Signatory, for individual certificates, or the future key holder, for organisation certificates, access to the certificate.
- If applicable, deliver the corresponding cryptographic device.
- Keep the documents provided by the applicant or Signatory on file for the period required by current law.
- Respect contract provisions signed with Camerfirma and with the Subject/Signatory.
- Inform Camerfirma about the causes for revocation, when known.
- Provide basic information about the certificate's policy and use, especially including information about Camerfirma and the applicable Certification Practices Statement, as well as their obligations, powers and responsibilities.
- Provide information about the certificate and the cryptographic device.
- Compile information and evidence about the certificate holder or receiver and, if applicable, the cryptographic device, and acceptance of such elements.
- Report on the attribution method exclusive to the private key holder and, if applicable, the cryptographic device's certificate activation data, according to this document's corresponding sections.

These obligations are even in cases of entities delegated by these such as points of physical verification.

The information about the Signatory's use and responsibilities is provided once the terms of use are accepted prior to the confirmation of the certificate application and via email.

The RAs' responsibility

The RAs sign a service provision agreement with Camerfirma, by virtue of which Camerfirma delegates registration duties to the RAs, which mainly consist of:

1.- Obligations prior to issuing a certificate.

- Informing applicants about signing their obligations and responsibilities.
- Properly identifying applicants, who must be trained or authorised to request a digital certificate.
- Checking the validity of the applicant's details and the Entity's details, if there is a contractual relationship or powers of representation.
- Accessing the Registration Authority application to process requests and issued certificates.

2.- Obligations once the certificate has been issued.

- Signing Digital Certification Service Provision agreements with applicants. In most issuance processes, this contract is formalised by accepting the conditions on the websites that are part of the process of issuing the certificate. The certificate cannot be issued without the terms of use having previously been accepted.

- Maintaining the certificates while they are still in force (expiry, suspension, revocation).
- Filing copies of submitted documentation and the agreements signed by the applicants in accordance with the Certification Policies published by Camerfirma and current law.

Therefore, the RAs are responsible for any consequences due to non-compliance of registration duties, and undertake to adhere to Camerfirma's internal regulations (Policies and CPS), which the RAs must keep perfectly controlled and which they must use as guidelines.

In the event of a claim from a Subject, Entity or user, the CA must offer proof that it has acted diligently and if there is evidence that the cause of the claim is due to incorrect data validation or checking, the CA can hold the RA liable for the consequences, in accordance with the agreement signed with the RAs. Because, although legally the CA is the legal entity liable to the Subject, an Entity or User Party, and the Subject, an Entity or User Party has liability insurance, according to the current agreement and binding policies, the RA has a contractual obligation to "correctly identify and authenticate the Applicant and, if applicable, the corresponding Entity", and in virtue of this must respond to Camerfirma in the event of breach.

Of course, it is not Camerfirma's intention to burden the RAs with the entire weight of responsibility for any damages due to a breach of the duties delegated to the RAs. For this reason, in the same way as for the CAs, the RA is subject to a control system imposed by Camerfirma, not only based on checking the files and filing systems the RA receives, but also audits to evaluate the resources used and its knowledge and control over the operational procedures used to provide the RA services.

The same responsibilities are assumed by the RA in virtue of breaches of the delegated entities such as points of physical verification (PVP), without prejudice to their right to contest them.

### 9.6.3 Subscriber representations and warranties

#### 9.6.3.1 Signatory

A certificate's Signatory (either directly or via an authorised third party) undertakes to comply with legal provisions and to:

- Accept the terms and conditions imposed by the provider.
- Use the Signatory's information within the rules imposed by the Data Protection Act.
- Allow publication of digital certificates in a public repository.

- Provide the RA with the information required for proper identification.
- Ensure the accuracy and authenticity of the supplied information.
- Report any changes to the data provided to create the certificate during its validity period.
- Keep their private key secure.

#### 9.6.3.2 Subject/Certificate holder.

The Subject undertakes to comply with legal provisions and to:

- Use the certificate in accordance with this CPS and the applicable Certification Policies.
- Respect the provisions established in the documents signed with Camerfirma and the RA.
- Report any cause for suspension/revocation as soon as possible.
- Report any inaccuracy or change to the data provided to create the certificate during its validity period.
- Not to use the private key or certificate once Camerfirma or the RA requests or reports the suspension or revocation thereof, or once the certificate validity period has expired.
- Make personal and non-transferable use of the digital certificate and therefore assume responsibility for any action that contravenes this obligation and fulfil the obligations that are specific to the applicable regulations for such digital certifications.
- Authorise Camerfirma to process the personal data contained in the certificates in connection with the purposes of the digital relationship and, in any case, to meet the legal obligations of certificate verification.
- Ensure that all the information provided via any means, the license application and the information in the certificate is accurate, complete for the purpose of the certificate and current at all times.
- Immediately inform the certification corresponding service provider of any inaccuracies detected in the certificate once issued, as well as changes to the information provided for issuing the certificate.
- If the certificate is on a physical device, if it is lost, advise the entity that issued the certificate incontrovertibly and as soon as possible and in any event within 24 hours, regardless of the specific event that has occurred or actions that may eventually occur.
- Do not use the private key, the digital certificate or any other technical media delivered by the corresponding certification service provider to perform any transaction prohibited by applicable law.

In the case of qualified certificates, the Signatory or certificate holder must use the key pair exclusively for creating digital signatures or seals and in accordance with any other limitations reported.

The Signatory or certificate holder must be especially diligent in safeguarding their private key and its secure signature creation device, in order to prevent unauthorised use.

If Signatories generate their own keys, they undertake to:

- Generate the keys using an algorithm recognised as acceptable for digital signatures, qualified if applicable, or digital seal, if applicable qualified.
- Create the keys within the signature creation device or seal, using a secure device where appropriate.
- Use key lengths and algorithms recognised as acceptable for digital signatures, qualified if applicable, or digital seal, qualified if applicable.

#### 9.6.3.3 Entity

In the case of certificates involving a business relationship, the Entity undertakes to request suspension/revocation of the certificate from the RA when the Subject/Signatory ends its business relationship with the organisation.

### 9.6.4 Relying party representations and warranties

The User Party undertakes to comply with legal provisions and to:

- Check the validity of the certificates before undertaking any transaction based on them. Camerfirma has established various channels for this verification, such as access to revocation lists or online query services such as OCSP, all of which are described on Camerfirma's website.
- Become familiar with and adhere to the guarantees, limitations and responsibilities regarding acceptance and use of trusted certificates, and agree to be subject to them.

### 9.6.5 Representations and warranties of other participants

No stipulation

## *9.7 Exemption from liability*

In accordance with current law, the responsibility assumed by Camerfirma and the RA does not apply in cases in which certificate misuse is caused by actions attributable to the Subject and the User Party due to:

- Not having provided the right information, initially or later as a result of changes to the circumstances described in the digital certificate, when the certification service provider has not been able to detect the inaccuracy of the data.
- Having acted negligently in terms of storing the data used to create the signature and keeping it confidential;
- Not having requested the suspension or revocation of the digital certificate data in the event of doubts raised over their storage or confidentiality;
- Having used the signature once the digital certificate has expired;
- Exceeding the limits established in the digital certificate.
- Actions attributable to the User Party, if this party acts negligently, that is, when it does not check or heed the restrictions established in the certificate in relation to allowed use and limited amount of transactions, or when it does not consider the certificate's validity situation.
- Damages caused to the Subject or trusting third parties due to the inaccuracy of the data contained in the digital certificate, if this has been proven via a public document registered in a public register, if required.

Camerfirma and the RAs are not liable in any way in the event of any of the following circumstances:

1. Warfare, natural disasters or any other case of Force Majeure.
2. The use of certificates in breach of current law and the Certification Policies.
3. Improper or fraudulent use of certificates or CRLs issued by the CA.

4. Use of the information contained in the Certificate or CRL.
5. Damages caused during verification of the causes for revocation/suspension.
6. Due to the content of messages or documents signed or encrypted digitally.
7. Failure to retrieve encrypted documents with the Subject's public key.

## *9.8 Limitations of liability*

The monetary limit of the transaction value is expressed in the final entity's certificate by including the extension "***qcStatements***", (OID 1.3.6.1.5.5.7.1.3), as defined in **RFC 3039**. The monetary value expression shall be in keeping with section 5.2.2 of standard **TS 101 862** of the ETSI (European Telecommunications Standards Institute, www.etsi.org).

Unless the aforementioned certificate extension states otherwise, the maximum limit Camerfirma allows in financial transactions is 0 (zero) euros.

## *9.9 Indemnities*

See section 9.2 and 9.6.1

## *9.10 Term and Termination*

### 9.10.1 Term

See section 5.7.3

### 9.10.2 Termination

See section 5.7.3

### 9.10.3 Effect of termination and survival

See section 5.7.3

## *9.11 Individual notices and communications with participants*

Any notification in relation to this CPS shall be made by email or certified mail to any of the addresses listed in the contact details section.

## *9.12 Procedures specifying changes.*

### 9.12.1 Procedure for amendment

This CPS is amended when any significant changes are made to certificate management for any type of certificate to which it applies. Yearly reviews will take place should no changes have been made in that time. These reviews are included in the version table at the start of the document.

### 9.12.2 Changes with notice

#### 9.12.2.1 List of aspects

Any aspect of this CPS can be changed without notice.

#### 9.12.2.2 Notification method

Any proposed changes to this policy are published immediately on Camerfirma's website

http://www.camerfirma.com/area-de-usuario/politicas-y-practicas-de-certificacion/

This document contains a section on changes and versions, specifying the changes that occurred since it was created and the dates of those changes.

Changes to this document are expressly communicated to third party entities and companies that issue certificates under this CPS.

#### 9.12.2.3 Period for comments

The affected Subjects/Signatories and Trusted Third Parties can submit their comments to the policy management organisation within 15 days following receipt of notice. The Policies state 15 days

#### 9.12.2.4 Comment processing system

Any action taken as a result of comments is at the PA's discretion

### 9.12.3 Circumstances under which OID must be changed

Not stipulated

## *9.13 Dispute resolution procedure*

Any dispute or conflict arising from this document shall be definitively resolved by means of arbitration administered by the Spanish Court Arbitration in accordance with its Regulations and Statutes, entrusted with the administration of the arbitration and the nomination of the arbitrator or arbitrators. The parties undertake to comply with the decision reached.

## *9.14 Applicable legal regulations*

Camerfirma is obliged to fulfil the requirements established within **current Spanish and European Union law as** the trading company providing digital certification services (hereinafter, regulations or current law). This law is defined in the internal document “Compliance with legal requirements"

## *9.15 Compliance with applicable law*

See section 9.14

## *9.16 Miscellaneous provisions*

### 9.16.1 Complete Agreement

The Signers and third parties that rely on the Certificates assume in their entirety the content of this Certification Practices and Policy Statement.

### 9.16.2 Assignment

Parties to this CPS may not assign any of their rights or obligations under this CPS or applicable agreements without the written consent of Camerfirma

### 9.16.3 Separability

Should individual provisions of this CPS prove to be ineffective or incomplete, this shall be without prejudice to the effectiveness of all other provisions.
The ineffective provision will be replaced by an effective provision deemed as most closely reflecting the sense and purpose of the ineffective provision. In the case of incomplete provisions, amendment will be agreed as deemed to correspond to what would have reasonably been agreed upon in line with the sense and purposes of this CPS, had the matter been considered beforehand.

### 9.16.4 Compliance (attorneys' fees and exemption of rights)

No stipulation

### 9.16.5 Force majeure

Force Majeure clauses, if existing, are included in the “Subscriber Agreement”.

## *9.17 Other Provisions*

### 9.17.1 Policy publication and copy

An electronic copy of this CPS is available at:

http://www.camerfirma.com/area-de-usuario/politicas-y-practicas-de-certificacion/

### 9.17.2 CPS approval procedures

The publication of reviewed versions of this CPS must be approved by Camerfirma Management.

AC Camerfirma publishes each new version on its website. The CPS is published in PDF format digitally signed by AC Camerfirma SA management.