CERTIFICATION

PRACTICE

STATEMENT
DIGITAL CERTIFICATES
AC CAMERFIRMA SA

Version 3.3

FRANCE MARIE SYLVIA VIDAL LECA

Firmado digitalmente por FRANCE MARIE SYLVIA VIDAL LECA
Fecha: 2018.03.28 11:00:52 +02'00'

RAMIRO MUÑOZ MUÑOZ

Firmado digitalmente por RAMIRO MUÑOZ MUÑOZ
Fecha: 2018.03.28 09:16:58 +02'00'

Language: **English**
Date: December 2004

October 2004	v2.0	New Hierarchies. Inclusion of code signing policy. Errata correction v2.0
Mar 2004	V2.2	Inclusion of power of attorney, corporate digital seal and TSA certificates
June 2006	V3	Amendment to adapt the document to latest changes and to ISO17799. This document is valid as an LOPD (Data Protection Act) security document and as a Security document.
May 2007	V3.1	Expiry of certificates With Power of Attorney and Without Power of Attorney
December 2007	V3.1.1	Review of policies. (Amendment of key usage to include non repudiation in signing certificates.
May 2008	V3.1.2	Clarifications in corporate digital seal and code signing certificate validation process. Changes to types of certificates in RACER hierarchy with certification policy.
July 2008	V3.1.3	Inclusion of CA Corporate Server EV. Changes requested by E&Y for WEBTRUST audit
July 2008	V3.1.4	Inclusion of section on applicable legal regulations. Changes requested by E&Y for WEBTRUST audit
June 2009	V3.2	Complete review of wording, inclusion of EV certificates. Inclusion of OID RACER. Information about the new ROOT 2008 passwords. Civil Servant Certificate according to the development of Law 11/2007 LAECSP. Comments on validating the title-holder in the corporate digital seal. Signing of OCSP certificates by CA. Monthly validation of EV certificates.
February 2010	V3.2.1	Inclusion of the new intermediate CA for Public Administrations (point 1.2.1.1 point 5) Improved description of EV certificate issue process, required by Mozilla. General review. Amended description of the person responsible for the certificate (points 1.4.8 and 2.1.3). Corrections to CRL issue (point 2.6.2) Corrections to registration of CA Public Administrations (point 6.1.1) Add reference to HSM ncipher (points 6.1.8 and 6.2) Amendment 4.8. Amendment to 8.2.1
February 2011	V3.2.2	Review of E&Y WebTrust renovation audit process
March 2011	V3.2.3	Improved description of the definition of responsibilities of the parties involved in the certification system, especially Camerfirma and the RAs. 2.2. 2.5.5 Returns policy 3.1.8 Inclusion of authorisation in seal and code signing certificates. 4.5.4 Deletion of the revocation via SMS, which is no longer used. 5.2.2 Double validation of EV requests. Amendment of links to information on Camerfirma's web site.
September 2011	V3.2.4	Change to profile of field 1.3.6.1.4.1.17326.30.3 organisation's identification document number. The first two characters that denote the country are deleted in the individual, power of representation, power of attorney, encryption and electronic invoicing profiles.
March 2012	V3.2.5	Periodic Review. Improved wording, inclusion of references in technical documentation not included in this document. BR and EV adaptation by CA/B FORUM Changes to length of user passwords to 2048. Inclusion 3.1.4.1
June 2015	V3.2.7	General review. Changes to time stamp procedures

		Changes to the SSL issue process. Changes of address for the links on the WEB due to changing content manager. Correction in the table of contents. Informa has been added as a source of information for issuing component certificates. Self-Employed people have been added as applicants for component certificates. Review of seal and code signing process. Inclusion of the SubCA certificate issuing programme for third parties, either with internal or external resources. The hierarchy of the Government of Andorra has been added in ChamberSign Global Root. CGCOM Outdated certificate procedure for Vodafone mobile phones deleted. (4.3.2.3) Explanations have been added for issuing SAN certificates. 3.1.8.2.1 / 3.1.8.2.5 Centralised management of HSM passwords added. Corrections of WebTrust 2015.
September 2015	v.3.2.8	Modification INDECOPI (Perú Supervisor Body), 4.8.2 Causes of revocation: NEW : Signature resolution of the competent administrative or judicial authority.
December 2015	v.3.2.8	Text correction 6.2 about private key protection. Add Codesign OID.
July 2016	V3.2.9	Substitution of certificates of legal person for certificates of physical representation and electronic seals.
March 2018	v.3.3	1.2 clarification on the alignment of these practices with the Baseline Requirement of CA / B FORUM. 3.1.8.3.1 Incorporation of CAA checking in the validation process for Server certificates according to RFC 6844. 4.8.3 Revocation by third parties. Revocation in case of incorrect issuance (CA / BFORUM requirement). 1.5.4 Domain check delegation. 1.2.1.1 No test certificates for SSL/TSL

Table of Contents

1. Introduction

1.1. Initial Consideration

Given that there is no specific definition of the concepts of Certification Practice Statement and Certification Policies, and due to some confusion that has arisen, Camerfirma understands that it is necessary 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 Practice Statement (CPS) is defined as a set of practices adopted by a Certification Authority for issuing certificates. It usually contains detailed information about its certificate security, support, administration and issue system, as well as the trust relationship between the Signatory/Subscriber or Trusting Third Party and the Certification Authority. These may be completely comprehensible and robust documents which provide an accurate description of the services offered, detailed certificate life cycle management procedures, and so on.

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

A detailed Certification Practice 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 "**what**" security requirements are required for issuing certificates. **The Certification Practice Statement tells us "**how" the security requirements established in the Policy are fulfilled.

1.2. General Overview

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

- RCF 3647 – *Internet X. 509 Public Key Infrastructure Certificate Policy*, by IETF,
- RFC 3739 3039 IETF Internet X.509 Public Key Infrastructure: Qualified Certificates Profile.

- RFC 5280, RFC 3280: Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL).
- RFC 6960 Online Certificate Status Protocol – OCSP
- ETSI TS 101 456 V1.2.1 Policy requirements for certification authorities issuing qualified certificates
- ETSI TS 102 042 V1.1.1 Policy requirements for certification authorities issuing public key certificates
- ETSI TS 102 023 V1.2.1 Policy requirements for time-stamping authorities technically equivalent to RFC 3628
- CA/Browser Forum Baseline Requirements for issuing and managing Publicly Trusted Certificates.
- These practices are aligned with the requirements set out in the Baseline Requirements for the Issue and Management of Publicly-Trusted Certificates prepared by the CA / BROWSER FORUM http://www.cabforum.org in its version 1.5.4.

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 Electronic Signatures – Part 1: System Security Requirements* have also been taken into consideration.

In general, the certificates that are not eligible or recognised comply with the requirements that are set forth in the technical specification ETSI TS 102 042, for the NCP or NCP + policy when greater security guarantees are required.

The eligible certificates comply with the requirements that are set forth in the technical specifications ETSI TS 101 456, for the QCP public or QCP + SSCD policy when issued together with a secure device for creating electronic signatures.

This CPS is compliant with the Certification Policies for the different certificates that Camerfirma issues, which are established in section **1.2.1** of this CPS. In the event of any conflict between both documents, the provisions of this document shall prevail.

1.2.1 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 into different CAs.

> All the Certification Authorities (CAs) described herein can issue OCSP responder certificates. This certificate is used to sign and verify the OCSP service responses regarding the status of the certificates issued by these CAs.

Camerfirma manages two hierarchical structures:

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

In general, the names of the CAs in the certificates issued for them are modified on their expiry date to include the year of their issue. For example, the name of the "CA Express Corporate Server" CA may be observed, which has changed to "CA Express Corporate Server 2009". Nevertheless, their OID and their characteristics will remain the same, unless otherwise indicated in this CPS.

1.2.1.1 Issuing of SET test certificates and test certificates in general.

Camerfirma issues certificates for the regulatory entity in inspection processes or the registration of new certificates as well as application developers in integration processes or evaluation processes for their acceptance, certified with the real hierarchy but with fictitious data. Camerfirma includes the following information in the certificates, in such a way that third parties that it trusts can clearly assess that it represents a test certificate without accountability:

Name of the entity	[ONLY TESTS] ENTITY
National Tax Identification Number for entity	R05999990
Address (street/number) of the entity	ADDRESS
Post code	5001
Contact telephone number	902361207
Name	JUAN
First surname	CÁMARA
Second surname	ESPAÑOL
National Identification Number	00000000T

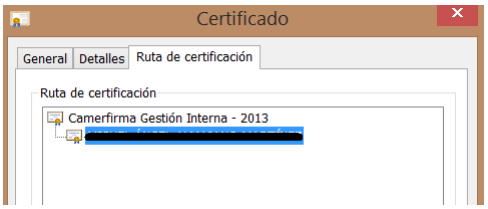
In cases where the approval, evaluation process... Requires a test certificate to be issued with real data, the process is carried out after the signing of a confidentiality agreement with the entity responsible for overseeing approval or evaluation tasks. The data is specified by each customer, but in front of the name of the entity [ONLY TESTS] always appears in order to identify at first glance that it is a test certificate without accountability.

No test certificates are issued for Website - SSL/TLS.

1.2.1.2 Hierarchy Camerfirma Internal Management.

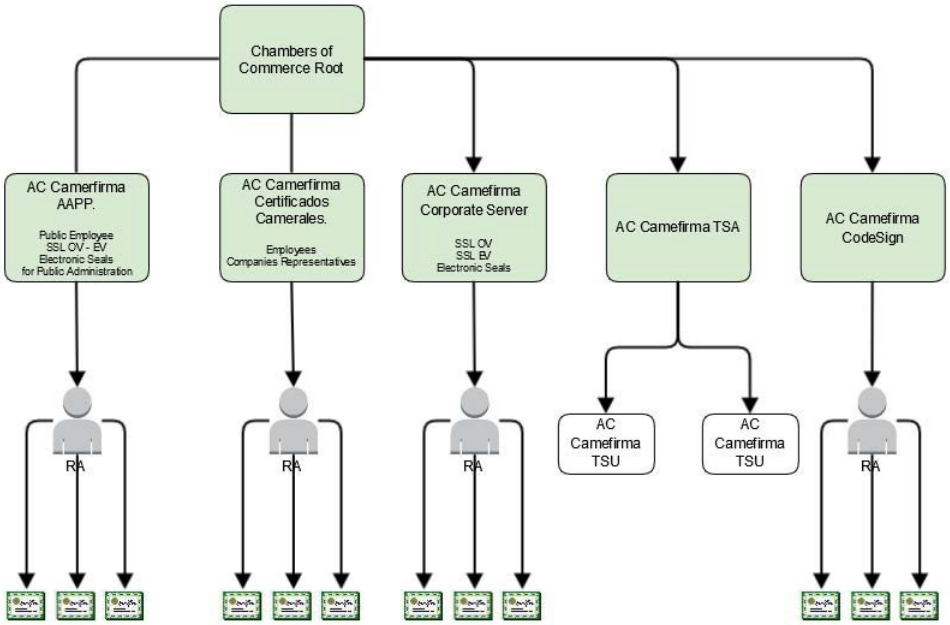
Camerfirma has developed a special certification authority for issuing operator certificates for entity registration. With this certificate an operator can oversee his/her own management tasks in accordance with his/her role on the Camerfirma STATUS® management platform.

This hierarchy is formed by a unique CA that issues the certificate to the end entity.



As a general design in the name of the certificate holder of the CAs that Camerfirma issues, the year of creation of the associated cryptographic passwords is included at the end of it, with its amendment being made in the corresponding year, in each certificate renewal process.

1.2.1.3 Hierarchy Chambers of Commerce Root.



(Chamber of Commerce Root) AnyPolicy

This Hierarchy is designed to develop a trusted network, with the ultimate aim of issuing corporate identity digital certificates 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: The component certificates (corporate digital seal, SSL, TSU, Code Signature) do not have any territorial limitations.
This hierarchy includes intermediate Certification Authorities that issue digital certificates

The characteristics of this hierarchy are summarised below:

- Spanish Geographical Scope. *(except for exceptions)*
- Registration Authorities managed by Chambers of Commerce.
- Business Scope.

in different environments:

CA Express Corporate Server.	AnyPolicy
Certificates for Secure server (OV)	1.3.6.1.4.1.17326.10.9.8
OCSP Responder	1.3.6.1.4.1.17326.10.12.2
AC Camerfirma CodeSign.	AnyPolicy
CodeSign	1.3.6.1.4.1.17326.10.12.2
OCSP Responder	1.3.6.1.4.1.17326.10.9.8
Time-stamping Authority (TSA).	AnyPolicy
TSU-2 Passwords in SW stored in HW. SmartTSU	1.3.6.1.4.1.17326.10.13.1.2
Time stamp TSU-2	1.3.6.1.4.1.17326.10.13.1.2.1
TSU-3 Passwords in HW with authenticated access to the service.	1.3.6.1.4.1.17326.10.13.1.3
Time stamp TSU-3	1.3.6.1.4.1.17326.10.13.1.3.1
OCSP Responder	1.3.6.1.4.1.17326.10.9.8
Camerfirma Corporate Server.	AnyPolicy
Certificates for Secure Server (EV)	1.3.6.1.4.1.17326.10.14.2
Corporate digital seal certificate.	1.3.6.1.4.1.17326.10.11.3
Certificates for Secure server (OV)	1.3.6.1.4.1.17326.10.11.2
OCSP Responder	1.3.6.1.4.1.17326.10.9.8
AC Camerfirma Chamber of Commerce Certificates	AnyPolicy
Contractual relationship with Entity.	1.3.6.1.4.1.17326.10.9.2
Powers of Representation.	1.3.6.1.4.1.17326.10.9.3
Special Power of Attorney.	1.3.6.1.4.1.17326.10.9.5
Legal entities.	1.3.6.1.4.1.17326.10.9.4
Electronic invoicing.	1.3.6.1.4.1.17326.10.9.7
Encryption.	1.3.6.1.4.1.17326.10.9.6
OCSP Responder	1.3.6.1.4.1.17326.10.9.8
AC Camerfirma AAPP	AnyPolicy
Electronic office, high-level.	1.3.6.1.4.1.17326.1.3.2.1
Electronic office, mid-level.	1.3.6.1.4.1.17326.1.3.2.2
Electronic Seal for Automated Procedures, high-level.	1.3.6.1.4.1.17326.1.3.3.1
Electronic Seal for Automated Procedures, mid-level.	1.3.6.1.4.1.17326.1.3.3.2
Public Employee, high-level, signature.	1.3.6.1.4.1.17326.1.3.4.1
Public Employee, high-level, authentication.	1.3.6.1.4.1.17326.1.3.4.2
Public Employee, high-level, encrypted.	1.3.6.1.4.1.17326.1.3.4.3
Public Employee, mid-level.	1.3.6.1.4.1.17326.1.3.4.4
OCSP Responder	1.3.6.1.4.1.17326.10.9.8

An updated list of this structure can be found on the Camerfirma website, in the section "Hierarchy Certification Practice and Policies"

1.2.1.3.1 Express Corporate Server.

The certificates issued by this CA will have continuity with the OID in the certification authority "Camerfirma Corporate Server – AAAA". AAAA represents the year of issue of the certificate.

This is an intermediate CA that issues digital certificates, the holders of which are machines or applications. This CA issues two different policies:

- **Certificates for OV (Organisation Validation) secure server** Issued to HTML web server applications via SSL/TLS or HTTPS protocol. This protocol is required to identify and establish secure channels between the user's or trusting third party's browser and the Signatory/Subscriber's HTML web server. ***The issue of this type of certificate complies with the requirements established by the document Baseline* Requirements for issuing and managing Publicly-Trusted Certificates *created by the CA/BROWSER FORUM http://www.cabforum.org*** using a policy identifier belonging to Camerfirma.

- **Corporate digital seal certificate**. This certificate is related to a key stored by a machine or application. Procedures that are carried out collectively are done automatically and without requiring assistance. The keys linked to the electronic seal certificate provide the documents and transactions to which it is applied with integrity and authenticity. It can also be used as client machine identification element in SSL/TLS or HTTPS secure communication protocols, and data encryption.

1.2.1.3.2 Code Signing.

The certificates issued by this CA will have continuity with the OID ones in the CA "Camerfirma Codesign – AAAA". AAAA represents the year of issue of the certificate.

Intermediate CA called **"Camerfirma CodeSign"** which issues certificates for code signing. As the name suggests, code signing certificates enable developers to apply an electronic signature to the code they have developed: ActiveX, Java applets, Microsoft Office macros, and so on, thus establishing the guaranteed integrity and authenticity of this code.

1.2.1.3.3 Time stamps.

The certificates issued by this CA will have continuity with the OID ones in the CA "Camerfirma TSA – AAAA". AAAA represents the year of issue of the certificate.

The third intermediate Authority **"AC Camerfirma TSA"** issues certificates for **issuing time stamps**. A time stamp is a data package with a standardised structure that associates the HASH code of a document or electronic transaction with a specific date and time.

The time stamp authority issues certificates to intermediate entities called "Time Stamp Units" **TSU**. These stamp units are responsible for ultimately issuing the time stamps upon the receipt of a standardised application that follows RFC 3161 specifications. Each one of these **TSUs** can be associated either to specific technical characteristics of the service or to exclusive use by a customer.

The TSU certificates have a duration of six years and a private key use of one year. Therefore the time certificates issued by these TSUs have a minimum duration of five years.

Under this DPC the issue of TSU certificates to companies and organisations that are located outside of Spanish territory is allowed. The procedure for issuing certificates is covered in the corresponding section in this DPC.

AC Camerfirma issues TSU certificates in **systems that are approved** by AC Camerfirma. The approved systems are published on the Camerfirma website. The approved systems can be located in the subscriber's installations under the signature of a affidavit and the compliance of the requirements associated with the issue of a TSU certificate.

AC Camerfirma also issues TSU certificates to be stored in **third party platforms** provided that these platforms:

- They are synchronised with the time sources established by Camerfirma.
- Allow Camerfirma or an authorised third party to audit the systems.
- Allow AC Camerfirma applications to access its stamp services with the aim of establishing the corresponding controls with respect to correcting the time stamp.
- Sign a service agreement.
- Allow AC Camerfirma access in order to gather information for the stamps issued or to send a periodic report for the number of stamps issued.
- Present a key creation document in a safe environment as is indicated in the Camerfirma TSA certification policies (HSM certified FIPS 140-1 Level 2) signed by a competent organisation. This document is previously assessed and signed by AC Camerfirma technical personnel before being deemed valid.

The TSU certificate policies are:

1.2.1.3.3.1 OID 1.3.6.1.4.1.17326.10.13.1.2.

The keys are created and stored on a certified, cryptographic set of cards EAL4+ CWA 14169. The key creation and storage process is recorded in the systems department, which is responsible for carrying out these operations.

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

1.2.1.3.3.2 OID 1.3.6.1.4.1.17326.10.13.1.3

The keys are created and stored in a HSM FIPFS 140-1 certificate, level 2 or higher.

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

1.2.1.3.4 Corporate Server. EV Secure Server.

The certificates issued by this CA will have continuity with the OID ones in the CA "Corporate Server – AAAA". AAAA represents the year of issue of the certificate.

This intermediate certification authority, **"AC Camerfirma Corporate Server EV"**, issues digital certificates for Secure Server or corporate electronic seals, with the same functions as the "Express Corporate Server" certification authority but subject to the requirements of the ***"CA/Browser Forum Guidelines for Issuance and Management of extended validation certificates"***. This regulation promotes the issue of secure server certificates with extra guarantees in the certificate holders' identification process. In this case, the name of the certification authority loses the word Express because the accreditation guarantees required for receiving the certificate are more demanding and therefore require a more elaborate procedure, resulting in a longer issuing time.

An EV Secure Server certificate provides browsers who connect to this service an extra level of guarantee; which they can see from the green background in the browser address bar.

Certificates issued up until this time by the "AC Camerfirma Express Corporate Server" CA are managed under this CA, using the same identification data from the OID policy.

1.2.1.3.5 AC Camerfirma Chamber of Commerce Certificates.

The certificates issued by this CA will have continuity with the OID ones in the CA "AC Camerfirma Chamber of Commerce Certificates – AAAA". AAAA being the year that the certificate is issued

"AC Camerfirma Chamber of Commerce Certificates" is a multi-policy Certification Authority that issues qualified or recognised business relationship certifications within Spain, pursuant to the criteria established in Law 59/2003, 19 December, on electronic signatures, the functions of which are described below.

The final certificates are intended for:

1.2.1.3.5.1 Natural persons with a business relationship with an Entity.

1.2.1.3.5.1.1 Contractual relationship with Entity.

These determine the type of contractual relationship (labour, mercantile, member of professional body, etc.) between a natural person (certificate holder/signatory/subscriber) and an Entity (organisation field in certificate).

1.2.1.3.5.1.2 Powers of Representation.

This determines the powers of legal representation or general power of attorney between the natural person (certificate holder/signatory/subscriber) and an Entity (also described in the Organisation field in the certificate).

1.2.1.3.5.1.3 Special Power of Attorney.

This determines the powers of specific representation or special power of attorney between the natural person (certificate holder/signatory/subscriber) and an Entity (also described in the Organisation field in the certificate).

1.2.1.3.5.1.4 Natural Person Qualified Certificate for Legal Person Representation in e-transactions with the Public Administrations.

It determines the legal representation relationship between the natural person (holder of the certificate / signatory / subscriber) and an Entity with legal personality (also described in the Organization field of the certificate).

1.2.1.3.5.1.5 Natural Person Qualified Certificate for Entity Representation without Legal Personality in e-transactions with the AAPP.

It determines the relationship of legal representation between the natural person (holder of the certificate / signatory / subscriber) and an Entity with legal personality (also described in the Organization field of the certificate).

1.2.1.3.5.1.6 Natural Person Qualified Certificate for Legal Entity Proxy Representative.

It determines the relationship of legal representation between the natural person (holder of the certificate / signatory / subscriber) and an Entity (described in the Organization field of the certificate).

1.2.1.3.5.2 Legal entities. (Cessation of issue from July 1, 2016).

The Legal Entity's digital certificate is created pursuant to **Law 59/2003**, Electronic Signatures, 19 December.

Camerfirma issues these certificates for documents that consist of the relationship between the Entity (Legal entity) and the Public Administrations (fiscal relations, electronic invoice issue, etc.) and, in general, as is determined in the current, applicable legislation for those proceedings that constitute the ordinary bank orders or dealings of the Entity, without prejudice to the possible quantitative or qualitative limits that may be added.

"Camerfirma mainly issues these certificates for tax purposes, allowing companies to conduct online procedures with the Spanish Tax Office. Outside of this scope, Camerfirma considers these certificates to be similar to the corporate digital seal and the Third Party that it trusts shall assess the use of the signature associated with this type of certificate as such." A seal guarantees the related document's authenticity and integrity."

In the case of a Legal Entity certificate, the holder/subscriber/signatory is the Entity itself, although it can only be applied for by one of the Entity's legal or voluntary representatives with sufficient powers for this purpose, who acts as custodian of the keys and as the person responsible for any actions undertaken with this certificate. ***However, contractually, and pursuant to the provisions of Law 59/2003, and without prejudice to the responsibilities that apply to the holder and applicant of the certificate, and which the holder or applicant subsequently assume, the certificate holder, if considered convenient to do so, will be able to transfer the use of the keys to a third party or to be included in an IT application, in order to meet each user's common practice needs of. In these cases in which the keys are transferred, the responsibility for their use continues to be assumed by the holder, without any kind of limitation.***

1.2.1.3.5.3 Electronic invoicing.

Electronic invoicing has been one of the means of promoting the use of electronic certificates. The Tax Agency regulates the use of the electronic certificates in the Royal Decree 1496/2003. In order to create an electronic invoice, it is necessary to sign the electronic document with an acknowledged certificate. Through the invoice certificate, Camerfirma creates a document adapted to the specific needs of electronic invoicing. The certificate is issued to a natural person who the Entity expressly authorises, and its use is limited to electronic invoicing.

1.2.1.3.5.4 Encryption.

Encryption certificates are technical certificates for the **exclusive** use of data encryption.

The aforementioned certificates (natural person with a relationship with entity, powers of representation, special power of attorney, electronic invoicing and legal entity) allow the key to be used for data encryption, but Camerfirma does not keep or store the private keys belonging to the certificate holders, pursuant to the requirements of **Law 59/2003** on Electronic Signatures, of 19 December. In this situation, if the certificate holder or, in the case of the legal entity certificate, the certificate custodian, loses control of the private key, access to all of the encrypted data with the related public key will also be lost.

The encryption certificate allows the service provider, in this case, Camerfirma, to look after the certificate holder's private key in order to be able to retrieve it in the event that it is lost.

1.2.1.3.6 AC Camerfirma AAPP.

The certificates issued by this CA will have continuity with the OID ones in the CA "Camerfirma AAAP-AAAA". AAAA being the year that the certificate is

issued

Law 11/2007, 22 June, on Citizens' Electronic Access to Public Services (LAECSP), Chapter Two, Heading Two, establishes the methods of application for identification and electronic signing via electronic certificates.

This Law provides various solutions to many problems that currently exist in relation to identification and electronic signing for Public Administrations, including with citizens and companies, and public sector employees.

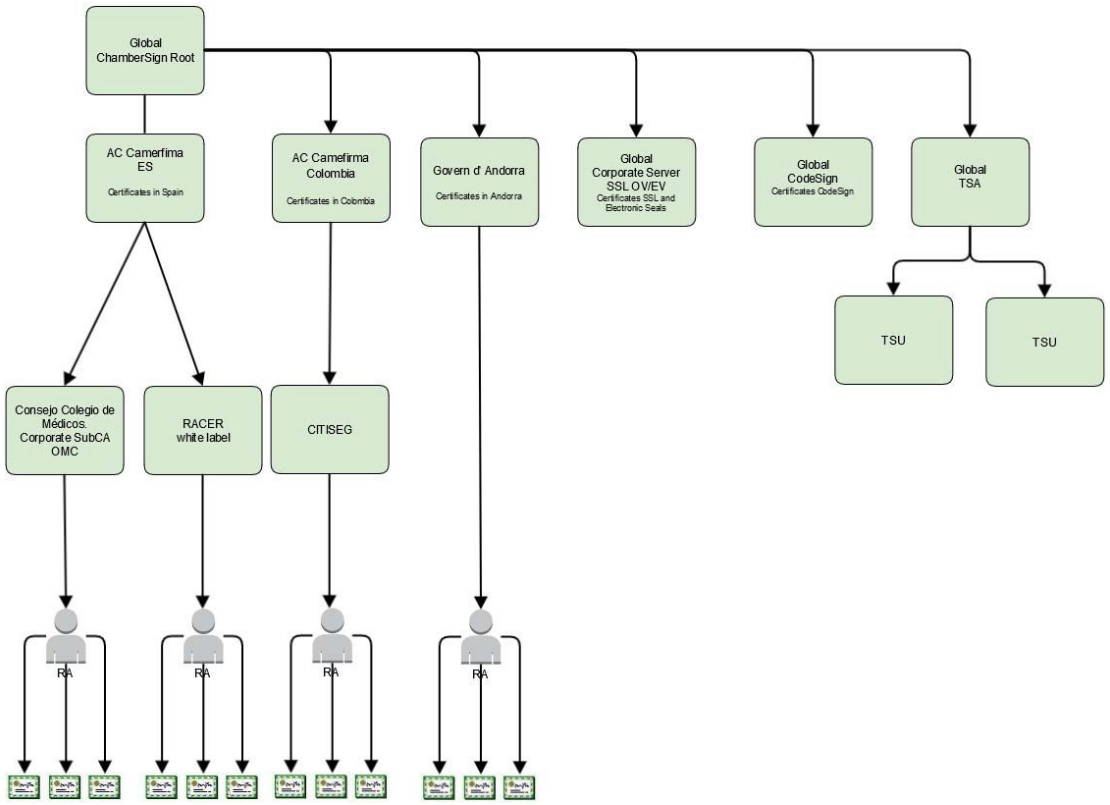
The General State Administration has defined a certification model that includes public certification service providers as well as the possibility of dependent bodies on the General State Administration being able to hire private certification service providers.

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

Pursuant to the foregoing and the Public Administration identification and signing system, and specifically its certification policy, AC Camerfirma issues the following types of certificates:

- Recognised Electronic Seal for Automated Procedures Certificate, high-level.
- Recognised Electronic Seal for Automated Procedures Certificate, high-level.
- Recognised Public Employee Certificate, high-level, signature.
- Recognised Public Employee Certificate, high-level, authentication.
- Recognised Public Employee Certificate, high-level, encryption.
- Recognised Public Employee Certificate, mid-level.
- Electronic office, mid-level.
- Electronic office, high-level.
- Public Employee-MID-LEVEL HARDWARE Smart Card Logon

1.2.1.4 Hierarchy Global Chambersign ROOT.



(Global ChamberSign Root) AnyPolicy

This hierarchy is created for the issue of certificates for specific projects with a specific Entity or specific Entities. It is therefore an open hierarchy in which certificates and their management are in keeping with the specific project needs. In this sense, and unlike the previously explained "Chamber of Commerce Root", the Registration Authorities are not necessarily included within the scope of the Spanish Chambers of Commerce, or within a specific regional scope, specific business scope or a business relationship.

Global Chambersign Root can also issue SubCA certificates to third party entities under the conditions described in the sections corresponding with this CPS.

The aim of this hierarchy is to develop a replicable model in different countries.

The main characteristics of this hierarchy are:

- UNRESTRICTED geographical scope
- UNRESTRICTED Registration Authorities.
- UNRESTRICTED scope in a business relationship.

In the scope of this hierarchy, different intermediate Certification Authorities are developed that correspond with different national scopes. The first intermediate Authority corresponds with AC Camerfirma SA (Spain) and within this Certification Authority:

- **AC Camerfirma (Spain)** AnyPolicy
    - **RACER (Spain)** AnyPolicy

Natural person with Business Relationship, Contractual Relationship Certificate	1.3.6.1.4.1.17326.10.8.2
Natural person with Business Relationship, Contractual Relationship Certificate	1.3.6.1.4.1.17326.10.8.3
Legal entity Certificate	1.3.6.1.4.1.17326.10.8.4
Electronic Seal Certificate	1.3.6.1.4.1.17326.10.8.5
Natural person for Entrepreneurial Citizen Certificate	1.3.6.1.4.1.17326.10.8.6
Natural person with Business Relationship, Electronic Invoicing Certificate.	1.3.6.1.4.1.17326.10.8.7
Natural person with Business Relationship, Power of Attorney Certificate	1.3.6.1.4.1.17326.10.8.8
Natural person Encryption Certificate	1.3.6.1.4.1.17326.10.8.9

    - **Certificate Entity OMC Organisation of Medical Colleges (Spain) – Own DPC/CPS** Any Policy.

College business certificate for identification purposes.	1.3.6.1.4.1.26852.1.1.1.1
College business certificate for signature.	1.3.6.1.4.1.26852.1.1.1.2
College business certificate for encryption	1.3.6.1.4.1.26852.1.1.1.3
College business certificate in software, for identification purposes, signature and encryption.	1.3.6.1.4.1.26852.1.1.7
College business certificate in HSM, for identification purposes, signature and encryption.	1.3.6.1.4.1.26852.1.1.9
Business certificate for administrative personnel for identification purposes.	1.3.6.1.4.1.26852.1.1.2.1
Business certificate for administrative personnel for signature.	1.3.6.1.4.1.26852.1.1.2.2
Card encryption certificate, for administrative personnel.	1.3.6.1.4.1.26852.1.1.2.3
Business certificate for administrative personnel, in software, for identification purposes, signature and encryption.	1.3.6.1.4.1.26852.1.1.1.6
Business certificate for a legal entity for identification purposes.	1.3.6.1.4.1.26852.1.1.3.1
Business certificate for a legal entity for signature.	1.3.6.1.4.1.26852.1.1.3.2
Card encryption certificate, for a legal entity.	1.3.6.1.4.1.26852.1.1.3.3
Business certificate for a legal entity in software, for identification purposes, signature and encryption.	1.3.6.1.4.1.26852.1.1.1.5

- **Global Chambersign CodeSign.** AnyPolicy.
- **Global Chambersign Corporate Server.** AnyPolicy.
- **Global Chambersign TSA.** AnyPolicy.

- **Andorra Public Administration Certification Entity** DPC/CPS Own AnyPolicy.

INDIVIDUAL in DSCF – SIGNATURA	2.16.20.2.1.3.1.1.3
INDIVIDUAL in DSCF – IDENTITAT	2.16.20.2.1.3.1.1.1
INDIVIDUAL in programari	2.16.20.2.1.3.1.1.2
PF INDIVIDUAL de ciutadà andorrà in DSCF – SIGNATURA	2.16.20.2.1.3.1.1.3
PF INDIVIDUAL de ciutadà andorrà in DSCF – IDENTITAT	2.16.20.2.1.3.1.1.1
INDIVIDUAL de ciutadà andorrà in programari	2.16.20.2.1.3.1.1.2
PROFESSIONAL INDIVIDUAL in DSCF – SIGNATURA	2.16.20.2.1.3.1.12.3
PROFESSIONAL INDIVIDUAL in DSCF – IDENTITAT	2.16.20.2.1.3.1.12.1
PROFESSIONAL INDIVIDUAL in programari	2.16.20.2.1.3.1.12.2
PROFESSIONAL INDIVIDUAL COL·LEGIAT in DSCF – SIGNATURA	2.16.20.2.1.3.1.12.3
PROFESSIONAL INDIVIDUAL COL·LEGIAT in DSCF – IDENTITAT	2.16.20.2.1.3.1.12.1
PROFESSIONAL INDIVIDUAL COL·LEGIAT in DSCF – XIFRAT	2.16.20.2.1.3.1.11.1
PROFESSIONAL INDIVIDUAL COL·LEGIAT in programari	2.16.20.2.1.3.1.12.2
INDIVIDUAL al servei d'una ORGANITZACIÓ in DSCF – SIGNATURA	2.16.20.2.1.3.1.4.3
INDIVIDUAL al servei d'una ORGANITZACIÓ in DSCF – IDENTITAT	2.16.20.2.1.3.1.4.1
INDIVIDUAL al servei d'una ORGANITZACIÓ in programari	2.16.20.2.1.3.1.4.2
INDIVIDUAL al servei de l´ADMINISTRACIO in DSCF – SIGNATURA	2.16.20.2.1.3.1.5.3
INDIVIDUAL al servei de l´ADMINISTRACIO in DSCF – IDENTITAT	2.16.20.2.1.3.1.5.1
INDIVIDUAL al servei de l´ADMINISTRACIO in DSCF – XIFRAT	2.16.20.2.1.3.1.11.1

INDIVIDUAL al servei de l'ADMINISTRACIO in programari	2.16.20.2.1.3.1.5.2
SEGELL D'EMPRESA (Legal entity) in HSM – Segell Electrònic	2.16.20.2.1.3.1.2.3
SEGELL D'EMPRESA (Legal entity) in HSM – IDENTITAT	2.16.20.2.1.3.1.2.1
SEGELL D'EMPRESA (Legal entity) in programari	2.16.20.2.1.3.1.2.2
REPRESENTANT INDIVIDUAL in DSCF – SIGNATURA	2.16.20.2.1.3.1.12.3
REPRESENTANT INDIVIDUAL in DSCF – IDENTITAT	2.16.20.2.1.3.1.12.1
REPRESENTANT INDIVIDUAL in programari	2.16.20.2.1.3.1.12.2
REPRESENTANT INDIVIDUAL in HSM – Segell Electrònic	2.16.20.2.1.3.1.3.3
REPRESENTANT INDIVIDUAL in HSM – IDENTITAT	2.16.20.2.1.3.1.3.1
REPRESENTANT INDIVIDUAL in programari	2.16.20.2.1.3.1.3.2
Govern d'Andorra TSA – Software – keys created by the PSC	2.16.20.2.1.3.1.13.1
Certificat d'actuació d'Administració, Òrgan o Entitat de Dret Públic in HSM	2.16.20.2.1.3.1.8.3
Certificat d'actuació d'Administració, Òrgan o Entitat de Dret Públic in programari	2.16.20.2.1.3.1.8.2

- **AC Camerfirma Colombia 2014**
  - **AC Camerfirma Colombia Type A – 2014 Any Policy.**

Legal entity Certificate	1.3.6.1.4.1.17326.20.1.3.*
Natural Person Certificate.	1.3.6.1.4.1.17326.20.1.4.*
Certificate belonging to Company.	1.3.6.1.4.1.17326.20.1.5.*
Corporate Representative Certificate.	1.3.6.1.4.1.17326.20.1.7.*
Professional Qualification Certificate.	1.3.6.1.4.1.17326.20.1.6.*
Public Role Certificate.	1.3.6.1.4.1.17326.20.1.2.*
Academic Community Certificate.	1.3.6.1.4.1.17326.20.1.1.*
Time Stamp Certificate	1.3.6.1.4.1.17326.20.2.1.*

1.2.1.4.1 AC Camerfirma

The certificates issued by this CA will have continuity with the OID ones in the CA "AC Camerfirma – AAAA". AAAA being the year that the certificate is issued

The purpose of this intermediate CA is to issue sector-specialised CA certificates (Banking, Health, etc.). To date, only one **general-purpose generic-brand** CA has been developed under this CA, called RACER.

1.2.1.4.1.1 CA RACER (acronym translated into English, High Capillarity Network of Registration Authorities)

The certificates issued by this CA will have continuity with the OID ones in the CA "RACER – AAAA". AAAA represents the certificate's year of issue.

The main characteristic of RACER is that it can be used by any agent as a Registration Authority, provided that the agent has previously received suitable training and has been subject to a registration process and auditing that verifies it is in a position to suitably comply with the "obligations" stipulated in the corresponding Certification Policies.

Also under this **CA**, natural person certificates can be applied for that do **not determine** the natural person's relationship or association with a legal entity and always guarantees the his or her identity as the Signatory/Subscriber, holder of the certificate.

RACER's policies do not define a specific regional scope, meaning that it can issue certificates anywhere there is a recognised RA that meets Camerfirma's established requirements, and ***always subject to current, applicable law and pursuant to international trading relations.*** However, the development of the Hierarchy Chambersign Global Root organises the issue of digital certificates in different countries by establishing the certification authorities expressly created for issuing certificates in a specific country and therefore better adapted to the legal framework and specific regulations.

1.2.1.4.1.2 CA of the Organisation of Medical Colleges. (OMC)

This CA is constituted under the hierarchy of the Global Chambersign Root for issuing certificates within the scope of the Organisation of Medical Colleges, the latter being established as the service provider for certification under Spanish legislation and has the Ministry for Industry as a national regulatory agency.

The particular characteristics of this Certification Authority makes it necessary for an independent document for AC Camerfirma SA general certification practice to be created. This practice document is available upon request by writing to juridico@camerfirma.com.

1.2.1.4.2 AC Global Chambersign Corporate Server AAAA.

The certificates issued by this CA will have continuity with the OID ones in the CA "AC Chambersign Corporate Server – AAAA". AAAA represents the certificate's year of issue.

This certification authority is created for issuing component certificates (Electronic Stamp, Secure Server SSL, OV, EV).

1.2.1.4.3 AC Global Chambersign CodeSign AAAA.

The certificates issued by this CA will have continuity with the OID ones in the CA "AC Chambersign Corporate Server – AAAA". AAAA represents the certificate's year of issue.

This certification authority is created for the issuing of component certificates (Code signing).

1.2.1.4.4 AC Global Chambersign TSA AAAA.

The certificates issued by this CA will have continuity with the OID ones in the CA "AC Chambersign Corporate Server – AAAA". AAAA represents the certificate's year of issue.

This certification authority is created for issuing TSU certificates.

1.2.1.4.5 AC Camerfirma Colombia XXXX.

The certificates issued by this CA will have continuity with the OID ones in the CA "AC AC Camerfirma Colombia – AAAA". AAAA represents the certificate's year of issue.

This CA, which belongs to AC Camerfirma, operates under the hierarchy of Global Chambersign Root for issuing certificates from the Certification Authority in Colombia under the Colombian legal framework.

This CA issues certificates to other Certification Entities that operate in Colombian territory.

Under this CA the second level CA CITISEG-XXXX operates, which issues final entity certificates. This CA belongs to CITISEG, a company formed in Colombia to undertake service provision activities for certification under the corresponding Colombian regulatory agency.

The particular characteristics of this Certification Authority makes it necessary for an independent document for AC Camerfirma SA general certification practice to be created. This practice document is available upon request by writing to juridico@camerfirma.com.

1.2.1.4.6 Certification Entity of the Andorra Public Administration.

Following the guidelines of the hierarchical organisation, this certification authority has been created with the aim to issue certificates in the geographical scope of the Principality of Andorra.

In general, the public hierarchy of certification of Andorra includes:

- The issue of certificates in the public sector of Andorra and to the citizens of Andorra, who are understood as the legal entities or natural persons of Andorran nationality or with legal residence in Andorra.
- The admission of certificates for the citizens of Andorra and foreigners who are not residents in Andorra, in their electronic relations with the public sector of Andorra.

For the purposes of this document, the public sector must be understood as:

- The Public Administration, as is defined in Article 13 of the Administration Code:
- The Executive Board and the governing bodies that are under their management.
- The common ones and areas and the governing bodies that depend on it.
- The independent entities or parapublic entities.
- The public corporations, with shares held by the Public Administration.

Depending on the use of the certificates, the following classification is established for them:

- Electronic signature certificates, which allow their use for the authentication of documents on behalf of a natural person, in agreement with the definition contained in Article 7, Law 6/2009, 29 December, regarding electronic signatures. Certificates can be ordinary or qualified.

  In general, ordinary certificates comply with the requirements that are set forth in the technical specification ETSI TS 102 042, for the NCP or NCP + policy, when higher level security guarantees are required.

  Qualified certificates comply with the requirements that are set forth in the technical specification ETSI TS 101 456, for the QCP public or QCP + SSCD policy, when they are issued together with a secure device for creating electronic signatures.

- Electronic seal certificates, which allow their use for the authentication of documents on behalf of a legal entity.

  In general, the electronic seal certificates comply with the requirements that are set forth in the technical specification ETSI TS 102 042, for the NCP or NCP + policy, when higher level security guarantees are required.

- Electronic identity certificates, which allow their use for the electronic identification of a natural person or legal entity.

  In general, the identity certificates comply with the requirements that are set forth in the technical specification ETSI TS 102 042, for the NCP or NCP + policy, when higher level security guarantees are required.

- Encryption certificates, which allow their use in order to guarantee the confidentiality of documents and the transfer of data.

  In general, encryption certificates comply with the requirements that are set forth in the technical specification ETSI TS 102 042, for the NCP policy.

Depending on the acquirer of the certificates, this policy establishes the following classification:

- Public corporate certificates, acquired on behalf of the public sector to cover their security needs.

- Citizenship certificates, issued by the Andorran Public Administration Certification Entity, or on behalf of other service providers of certification, when they have been submitted on behalf of the Public Administration.

The particular characteristics of this Certification Authority makes it necessary for an independent document for AC Camerfirma SA general certification practice to be created. This practice document is available in Spanish and Catalan upon request by writing to juridico@camerfirma.com.

1.3. 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 is therefore in the Policy Authority (PA) of the Certification Hierarchies and Authorities described above and is responsible for managing the CPS.

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

E-mail:	juridico@camerfirma.com The postal addresses, telephone and fax numbers are published on https://www.camerfirma.com/address

As far as the content of this CPS is concerned, it is assumed that the reader is familiar with the basic concepts of PKI, certification and digital signing. Should readers not be familiar with these concepts, they are advised to gain some background knowledge on them for example on the Camerfirma website http://www.camerfirma.com where there is general information about the use of digital signing and digital certificates.

1.4. Identification

Name:	CPS Camerfirma SA
Description:	Document to fulfil requirements of Policies with identification: See section 1.2.1.2 and 1.2.1.1
Version:	3.2.6
OID	1.3.6.1.4.1.17326.10.1
Location:	https://policy.camerfirma.com/

1.5. Community and Scope of Application.

1.5.1 Certification Authority (CA).

It is the component of a PKI that is responsible for issuing and managing digital certificates. It acts as the trusted third party between the Signatory (Subscriber) and the trusting third party in electronic transactions, linking a specific public key with a person.

A Certification Authority (CA) uses Registration Authorities (RA) to carry out the tasks involving the checking and sorting of the documentation from the content included in the digital certificate.

A CA belongs to a legal entity indicated in the organisation field (O) of the associated digital certificate.

The information concerning the CAs managed by Camerfirma can be found in this document or on the Camerfirma website http://www.camerfirma.com

More than one intermediate may exist between the root certification authority and the certificate from the final entity. The number of intermediate CAs allowed is specified in the Basic Constraints extension (pathLenConstraint) of the certificate from the Certification Authority.

1.5.1 Intermediate or subordinate Certification Authority (SubCA).

An intermediate Certification Authority (SubCA) is a hierarchical target that obtains a certificate from the Root CA in order to issue certificates from the final entity or other certificates from the CA. The SubCAs allow risks to be distributed in a complex hierarchical structure, allowing the latter to manage for example its keys in an "online" and more accessible environment, protecting the keys from the Root CA stored in a safe offline environment. A SubCA allows the organisation of different types of certificates issued by the main CA.

The certificate from a SubCA is signed by a root CA (root entity deriving from the certification hierarchy) or another SubCA.

A SubCA can be subject to limitations by the CA, on which it depends hierarchically. Technically through a combination of the following parameters within the certificate: Extended Key Usage and Name constraints additionally to those contractually established.

An intermediate Authority can be identified as internal or external. An internal SubCA belongs to the same organisation as the CA on which it depends hierarchically, in this case, AC Camerfirma. On the contrary, an external SubCA belongs to a different organisation, which has applied to be included in the hierarchy of the CA on which it depends hierarchically, and which may or may not use a technically different infrastructure.

1.5.2 Accreditation Authority

The accreditation authority accepts, authorises and supervises the certification authorities. This task falls to the Spanish government's Ministry for Industry, Tourism and Commerce, which is the competent authority depending on the Spanish Member State of the European Economic Area, pursuant to the legislation stipulated in compliance with the European Parliament and Council 1999/93/CE Directive, 13 December, by means of which a community framework is established for electronic signatures.

The SubCAs that Camerfirma develops may be subject to legal frameworks from different countries or regions, the accreditation entity in such circumstances corresponding with the corresponding national agencies.

- For Spain: Ministry for Industry, Energy and Tourism. http://www.minetur.gob.es
- For Colombia: National Accreditation Agency of Colombia (http:// http://www.onac.org.co/) allocated by the Colombian State Government
- For Andorra: Ministeri d'Economia and Territori del Govern d'Andorra
- Peru: National Defence Institute for the Scope and Protection of Intellectual Property (Indecopi http://www.indecopi.gob.pe/) affiliated with the Council Presidency of the Ministries of the State Government of Peru.
- Mexico: Secretary for the Economy of the Executive Authority of the Mexican United States.

1.5.3 Certification Service Provider (CSP).

It is understood that under this CPS, to a CSP such as that entity, a trusted third party, which provides specific services associated with the life cycle of the certificates and that may directly or indirectly manage one or more Certification Authorities and associated services, such as the issue of time stamps, providing signature devices or validation services.

AC Camerfirma issues SubCA certificates to third parties for their accreditation within and outside of the Spanish legal framework. These parties may be considered as a CSP in the said countries before their national accreditation entities.

1.5.4 Registration Authority (RA)

An RA can be a natural person or a legal entity that acts in accordance with this CPS, and, if applicable, by means of an agreement signed with a specific CA, exercising the management tasks for the application, identification and recording of the certificate applicants and those that are generated in the Certification Policies. RAs are authorities delegated by the CA, although the latter is ultimately responsible for the service.

The following types of RA are recognised under the present practice:

- **Chamber RA:** Those directly managed or under the control of a chamber of commerce.
- **Corporate RA:** Those managed by a public organisation or a private entity for the distribution of certificates to their employees. They are controlled by a Chamber RA in relation to the CA "Camerfirma Chamber of Commerce Certificates".
- **Remote RA:** Registration Authority managed in a remote location that is communicated with the platform through the STATUS WebServices layer.
- **OVP OVP** On-site Verification Point that always depends on an RA. Its main mission is to cover the evidence of the applicant's existence, and submitting documentation to the RA, which shall validate it according to the applicable Policy, in order to process the application for issuing the certificate. The OVP is not subject to training or controls for these functions.

  Sometimes, the OVP may expand its functions in cross-checking submitted documentation; checking its suitability with regards to the type of certificate applied for, as well as the delivery of the certificate to the applicant in the case of encrypted cards.

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

For the Chambers of Commerce Root Hierarchy:

- The Certification Authority.
- The Chambers of Commerce, Industry and Navigation, or the entities appointed by them. The registration process can be carried out on behalf of the different delegated entities:
- The Business Registration Authorities (Business RA), as entities delegated by a RA, to which they are contractually bound, in order to carry out the complete registrations of Signatories/Subscribers within a certain organisation or demarcation. In general, the operators of the said Business RAs shall solely manage the applications and the certificates in the scope of their organisation or demarcation, unless it is determined in another way by the RA that they depend on. For example, a corporation's employees, members of a corporate group, members of a professional body.
- The Public Administration, in the case of certificates issued under the **AC Camerfirma Public Administrations**.
- Any RA can delegate, in the On-site Verification Points (OVPs), the certificate-holder's on-site verification function and the receipt of documentation and, if applicable, the compiling of documentation and verification of its suitability as well as the delivery of material. In view of the fact that they do not have the ability to register, they are contractually bound with an RA by means of a contract that is provided

by Camerfirma. Based on the documentation supplied by the OVP, the RA operator checks the documentation and, if applicable the CA issues the certificate with no need to carry out a new on-site verification. The contract defines the functions delegated by the RA in the OVP.

For the Chambersign Hierarchy.

- The Certification Authority.
- Any national or international agent that has a contractual relationship with the CA and has passed the registration and audit processes established in the Certification Policies**.**

As is the case for the Chamber of Commerce Root hierarchy, the RA can delegate certain functions at the On-site Verification Points (OVPs) that are not related to the registration, such as the on-site verification of the certificate holder.

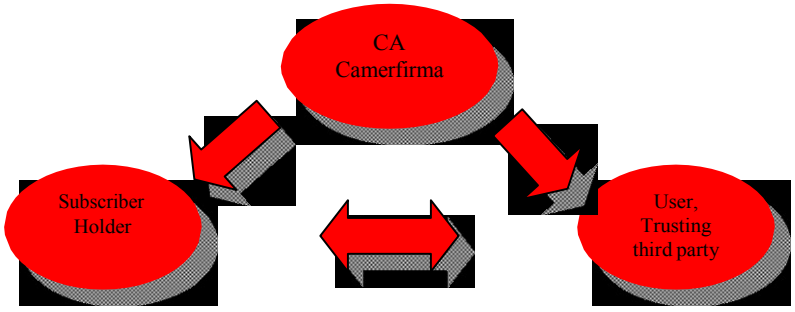
In any case is allowed to delegate domain validation process for a WebSite certificate.

1.5.5 Signatory/Subscriber.

The Signatory/Subscriber is the certificate holder, whether a natural person or a legal entity, and is described in the certificate's CN field. When it is issued in the name of a hardware device or software application, the natural person/legal entity applying for the issued certificate is considered the Signatory/Subscriber.

1.5.6 Trusting third party or certificate user.

In this CPS, the Trusting Third Party or user is the person receiving an electronic transaction carried out with a certificate issued by any of the Camerfirma CAs and who voluntarily trusts the Certificate that this CA issues. Chart.



1.5.7 Entity

An Entity is any public or private, individual or group company or organisation recognised by law, with which the Signatory/Subscriber has a certain relationship, which is defined in the ORGANISATION (O) field of each certificate.

And so

- ✓ In the case of the **Natural person or Public Employee Relationship certificate**, the Entity is bound to the Signatory/Subscriber by means of a mercantile, occupational, professional body, relationship etc.

- ✓ In **Powers of Representation certificates**, the Entity is represented by the Signatory/Subscriber who has broad powers of representation.

- ✓ In **Special Power of Attorney certificates**, the Entity is represented by the Signatory/Subscriber in specific procedures.

- ✓ In **Electronic invoicing** certificates, the Entity authorises the Signatory/Subscriber to issue electronic invoices.

- ✓ In the case of **Secure Server/Digital Seal**, **Electronic Website** certificates, the Entity owns the Internet domain or software for which the certificate has been requested.

- ✓ In **CodeSign certificates**, The entity linked to the procedure for which the signature is given.

- ✓ Other cases in other certificates (Andorra, CGCOM, Colombia, etc.), where the link with the Entity is that which can distinguish their respective certification practice.

As a general rule, the Entity is identified in the organisation (O) field in the certificate and its tax identification number is entered in a field for this purpose in the certificate. For further details, see section 3.1.1.

1.5.8 Applicant

The Applicant is the natural person applying for the Certificate from the Camerfirma CSP, either directly or through an authorised representative.

Applicants may be:

- The person who is the future signatory of the certificate.
- A representative from the organisation under whose name the certificate is issued.
- A person authorised by the future subscriber/signatory of the certificate.
- A person authorised by the Registration Entity.
- A person authorised by the Certification Entity.

1.5.9 Certificate Manager/Owner of the keys

This CPS considers that the certificate holder (the signatory/subscriber) is responsible for certificates issued to natural persons.

For the certificates issued to legal entities, this CPS considers the natural person making the application (the applicant) to be responsible for certificates issued to the legal entities. This person must be identified in the certificate, even if the application is made through a third party.

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

1.5.10 End User

End users are persons who obtain and use personal, legal entity, device and object certificates issued by the Certification Entities and, specifically, the following end users can be distinguished:

- The certificate applicants.
- The certificate subscribers or holders.
- The owners of keys.
- The persons responsible for verifying signatures and certificates.

1.5.11 Scope of Application and Usage.

This CPS fulfils the Certification Policies described in section 1.2 of this CPS.

Camerfirma certificates can be used pursuant to the terms and conditions set out in the Certification Policies.

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

- **Authentication** based on certificates X.509v3, pursuant to the corresponding electronic authentication policy.
- **Electronic signature**, advanced or recognised, based on X.509v3 certificates, pursuant to the corresponding electronic signature policy.
- **Asymmetric or mixed encryption**, based on X.509v3 certificates, pursuant to the corresponding encryption policy.

1.5.11.1 Prohibited and Unauthorised Use.

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

The certificates have not been designed, cannot be assigned and are not authorised for use or resale as control systems for dangerous situations or for uses that require fail-safe functioning, such as nuclear power plant operations, navigation systems or aviation communications, or weaponry control systems, where an error may directly result in death, personal injury or severe environmental damages.

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 Signatories/Subscribers are considered illegal, and the CA is exempt from any liability due to the signatory or third party's misuse of the certificates pursuant to current law.

Camerfirma does not have access to the data for which a certificate is used. Therefore, due to this technical impossibility of being able to access the message content, Camerfirma cannot issue any appraisal regarding this content, and the signatory is consequently responsible for the content linked to the use of the certificate. 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 Signatories, as well as any misuse thereof pursuant to this paragraph or which could be interpreted as such by virtue of current law.

Camerfirma includes information in the certificate with regards to the limitation of use, either in standardised fields in the attributes *key usage*, *basic constraints* and/or *name constraints* marked as critical in the certificate and therefore of obligatory compliance by the applications that use them, or even limitations in the attributes such as *extended key usage* and/or by means of text included in the *user notice* field indicated as "not critical" but of obligatory compliance by the certificate holder and user.

1.6. Applicable legal regulations

Camerfirma is obliged to fulfil the requirements established within **current Spanish 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"***

1.7. Contact

This CPS is managed by the Camerfirma legal department, which can be contacted via:

E-mail:	juridico@camerfirma.com C/ Ribera del Loira, 122 8042 MADRID Telephone: 902 361 207 +34 914 119 661 Web site with contact details https://www.camerfirma.com/address

2. General Clauses

2.1. Obligations

Pursuant to the stipulations of the Certification Policies and this CPS, and pursuant to current law regarding certification service provision, Camerfirma undertakes to:

- Respect the provisions 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 does 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 any legal provisions regarding data protection.
- Suspend and revoke certificates in accordance with this Policy and publish the revocations in the CRL.
- Inform Signatories/Subscribers about the revocation or suspension of their certificates, as and when due, pursuant to current law.
- Publish this CPS and the Certification Policies on its web site.
- Inform the Signatories/Subscribers and the RAs that are bound to them of any amendments to this CPS and the Certification Policies.
- Not to store or copy the data used to create the Signatory/Subscriber's signature, except for the encryption certificates.
- Protect the data used to create the signature while it is in its safekeeping, if applicable.
- Establish the data creation and custody systems in the aforementioned activities, protecting this data against being lost, destroyed or forged.
- Keep the data relating to the issued certificate for the minimum period required by current law.

2.1.1 External SubCA.

The external SubCAs are CAs included in the CA root hierarchy but which belong to a different organisation and may or may not use a different technical infrastructure.

- Protect their private keys.
- Issue certificates pursuant to the certification policies and/or corresponding CPS.
- Issue certificates free of errors.

- Publish the certificates in a repository that can be accessed by AC Camerfirma.
- Allow annual auditing.
- Keep all documented information and information in relation to the systems that have been used for creating and issuing certificates for the period of time that is established by current, applicable legislation.
- Notify AC Camerfirma of any incidents concerning the delegated activity.

2.1.2 RA

RAs are entities that Camerfirma appoints to carry out certificate application registration and approval tasks. Therefore, the RAs are also obliged under the terms defined in the Certification Practices for issuing certificates, and in particular to:

- ✓ Adhere to the provisions of this CPS and the Certification Policy.
- ✓ Protect their private keys that are used to carry out their functions.
- ✓ Check the identity of the Signatories/Subscribers of the certificates when it is deemed necessary, definitively accrediting the subscriber's identity, in the case of individual certificates, or the owners of keys, in the case of organisation certificates, pursuant to the provisions of the corresponding sections of this document.
- ✓ Check the accuracy and authenticity of the information provided by the Applicant.
- ✓ In the case of individual certificates, provide the subscriber or the future owner of keys, in the case of organisation certificates, with access to the certificate.
- ✓ Deliver, if applicable, the corresponding cryptographic device.
- ✓ Keep the documents provided by the applicant or subscriber on file for the period required by current law.
- ✓ Respect the provisions of the contracts signed with Camerfirma and with the Signatory/Subscriber.
- ✓ Inform Camerfirma about the causes for revocation, when these are known.
- ✓ Offer basic information about the policy and use of the certificate, in particular including information about Camerfirma and the applicable Certification Practice Statement, as well as its obligations, powers and responsibilities.
- ✓ Offer information about the cryptographic certificate and device.
- ✓ Gather information and evidence from the owner receiving the certificate and, if applicable, the cryptographic device, and acceptance of the said elements.
- ✓ Inform the owner of the private key of the exclusive allocation method and of their activation details for the certificate and, if applicable, of the cryptographic device, pursuant to the provisions of the corresponding sections in this document.

These obligations even in the cases of entities appointed by them such as the on-site verification points.

The information regarding the use and subscriber's responsibilities is supplied on acceptance of the provisions of use prior to confirmation of the certificate application and by e-mail.

2.1.3 Certificate applicant.

An applicant applying for a certificate (either directly or via an authorised third party) undertakes to comply with legal provisions and to:

- ✓ Provide the RA with the information required for correct 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.

2.1.4 Signatory/Subscriber.

The Signatory/Subscriber 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.
- ✓ During the validity period, report any errors or changes to the data provided to create the certificate.
- ✓ Not use the private key or certificate once Camerfirma requests or reports the suspension or revocation thereof, or once the certificate validity period has expired.

- Make use of the digital certificate as personal and non-transferable document and, therefore, assume the responsibility for any act that is carried out in breach of this obligation, as well as complying with the obligations specified in the applicable regulations for the said digital certificates.
- Authorise Camerfirma to proceed with processing the personal details contained in the certificates, in connection with the purposes of the electronic account, and in any case, to comply with the legal obligations for certificate verification.
- Assume the responsibility so that all information included by any means for the certificate application and in the certificate itself is accurate and complete for the purposes of the certificate and that it is kept up-to-date at all times.

- Immediately inform the corresponding certificate service provider of any inaccuracy in the certificate that may be detected once it has been issued, as well as informing them of any amendments that are made to the information supplied for the issue of the certificate.
- In the event of certificates in a data device, in the event of any loss, inform the entity that has issued the certificate of such a loss, in good faith and as soon as possible, and in any case within 24 hours from the loss occurred, regardless of the specific reason why such circumstances arose or the actions that may eventually have to be exercised.
- Do not use the private key, the electronic certificate or any other technical medium handed over by the corresponding certification service provider to carry out any transaction that is prohibited by applicable law.

In the case of qualified certificates, the subscriber or owner of certificates must use the pair of keys solely for creating electronic signatures or stamps and in compliance with any other limitations that they are notified with.

Similarly, particular care must be taken in the safekeeping of their private key and of the secure device for creating the signature, with the aim of avoiding any unauthorised use.

If subscribers creates their own keys, they are obliged to:

- Create their subscriber keys using an algorithm that is acknowledged as acceptable for the electronic signature, if applicable qualified, or the electronic stamp, if applicable qualified.
- Create they keys within the signature or stamp creation device, using a secure device if applicable.
- Use key lengths and algorithms that are acknowledged as acceptable for the electronic signature, if applicable qualified, or the electronic stamp, if applicable qualified.

2.1.5 Trusting third party/User.

The Trusting Third 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 consultation services such as OCSP, all of which are described on Camerfirma's website: http://www.camerfirma.com/area-de-usuario/consulta-de-certificados
- Become familiar with and adhere to the guarantees, limitations and responsibilities regarding the acceptance and use of the trusted certificates, and agree to be bound to them.

2.1.6 Entity

In the case of certificates involving a relationship with an Entity, the Entity is obliged to request suspension/revocation of the certificate from the RA when the Signatory/Subscriber ends its relationship with the Entity.

2.1.7 Repository

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

Repository of policies and certification practice.
http://www.camerfirma.com/area-de-usuario/jerarquia-politicas-y-practicas-de-certificacion-2/

This information is stored in a relational database with integrity and access measures to ensure it is stored in accordance with the Certification Policy requirements.

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

2.2. Responsibility.

Camerfirma's responsibility

Article 22.1 of the Law on Electronic Signatures establishes that: "*Certification service providers are responsible for damages and losses caused to any person during their activities in the event that they represent a breach in the obligations established in this Law.*
The certification service provider regulated herein shall be held liable pursuant to general regulations on contractual or non-contractual liability, as applicable, although the certification service provider must prove that it acted with due professional diligence."

Camerfirma shall be responsible for any damages or losses caused to the users of its services, whether the Signatory/Subscriber or Trusting Third Party, and other third parties pursuant to the terms and conditions established under current law and in the Certification Policies.

In this sense, Camerfirma is the only party responsible (i) for issuing the certificates, (ii) for managing them throughout their life cycle and (iii) if necessary, in the event of suspension and revocation of the certificates. Specifically, Camerfirma shall be 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 Signatory/Subscriber is in possession of the private key relating to the public key given or identified in the certificate when required, by using standard application 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 applied for and the certificate delivered match.
- Any liability established under current law.

Pursuant to current law, Camerfirma holds a public liability insurance policy that fulfils the requirements established in the certification policies affected by these certification practices.

Responsibility of the SubCA (Internal/External).

Without prejudice to Camerfirma's responsibility for issuing and revoking the digital certificates from the SubCAs as well as the contractual terms agreed on in each case, the SubCAs (through the legal entity on which they depend) are responsible for issuing and revoking digital certificates issued to end users, responding to subscribers and other third parties or users affected by the service, in agreement with their own Certification Practice Statements, Certification Policies and national legislation, if applicable.

The RA's responsibilities

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.
- Correctly identifying applicants, who must be trained or authorised to applying for 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 applications and issued certificates.

2.- Obligations once the certificate has been issued.

- Signing Digital Certification Service Provision agreements with applicants. In the majority of the issue processes, this contract is formalised by accepting the conditions on the website that form part of the certificate issue process. The certificate is not issued until the conditions of use have 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 pursuant to the Certification Policies published by Camerfirma and current law.

Thus, the RAs are responsible for any consequences due to any breach of or failure to correctly fulfil their registration duties, and by means of which they are obliged to adhere to Camerfirma's internal certification entity regulations (Policies and CPS), which must be perfectly controlled on behalf of the RAs and which must be used as a reference manual.

In the event of a claim from a Signatory, Entity or a user, the CA must provide 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, pursuant to the agreement signed with the RAs. Because, although legally it is the CA that is liable to the Signatory, an Entity or Trusted Third Party, and which for such a purpose has civil liability insurance, according to the valid agreement and the binding Policies, the RA is contractually obliged to "identify and correctly authenticate the Applicant and, if applicable, the corresponding Entity", and in its virtue shall answer to Camerfirma for its breaches.

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, the same as for the CAs, the RA is subject to a control system imposed by Camerfirma, not only by means of the file and safe-keeping procedure controls for the files received by the RA using audits to evaluate, among others, the resources used and the knowledge and control over the operational procedures used to provide the RA services.

The RA must assume the same responsibilities in virtue of breaches of the entities appointed, for example the on-site verification points (OVPs), without prejudice to their right to affect them.

2.2.1 Exemption from liability

Pursuant to 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 Signatory and the Trusting Third Party due to:

- Not having provided the correct information, initially or later as a result of changes to the circumstances described in the electronic 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 electronic certificate data in the event of doubts raised over its storage or confidentiality;
- Having used the signature once the electronic certificate has expired;

- Exceeding the limits established in the electronic certificate.
- Actions attributable to the Trusted Third Party, if this party acts negligently, that is, when it does not check or heed the restrictions established in the certificate in relation to its allowed use and limited number of transactions, or when it does not consider the certificate's valid status.
- Damages caused to the signatory or trusting third parties due to the inaccuracy of the data contained in the electronic certificate, if this has been proven via a public document registered in a public register, if required.

Camerfirma and the RAs are not responsible under any circumstances when the following circumstances arise:

1. Warfare, natural disaster or any other case of force majeure.
2. The use of certificates in breach of current law and the Certification Policies.
3. Unlawful or fraudulent use of the 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 Signatory's public key.

2.2.2 Limited responsibility in the event of losses due to transactions.

The monetary limit of the transaction value is expressed in the certificate of the final entity itself by including the extension "qcStatements", (OID 1.3.6.1.5.5.7.1.3), as defined in the RFC 3039. The monetary value expression shall be in keeping with the provisions of section 5.2.2 of the 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.

2.3. Financial responsibility

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 Signatory/Subscriber and the Trusted Third Party, and third parties, for a total amount of **€3,700,000.**

2.4. Interpretation and enforcement

2.4.1 Law

The enforcement, interpretation, amendment or validity of this CPS is subject to current Spanish law.

2.4.2 Independence

Should any of the clauses contained in this CPS be rendered invalid, the rest of the document shall not be affected. In such case, the aforementioned clause shall be considered not included.

2.4.3 Notification

Any notification in relation to this CPS must be made by email or certified mail to any of the addresses listed in the contact details section.

2.4.4 Dispute settlement procedure.

Any dispute or conflict arising from this document shall be definitively resolved by means of arbitration administered by the Spanish Arbitration Court pursuant to its Regulations and Statutes, entrusted with the administration of the arbitration and the nomination of the arbitrator or arbitrators. The parties agree to comply with the decision reached.

2.5. Prices

2.5.1 Price for certificate issue and renewal.

The prices for certification services or any other related services are available and updated on the Camerfirma website

http://www.camerfirma.com/certificados/ or upon request from the Camerfirma Support Department at https://secure.camerfirma.com/incidencias/ or by telephone 902 361 207.

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

2.5.2 Prices for access to certificates.

Access to certificates is free-of-charge, although AC Camerfirma applies controls to avoid mass certificate downloads. Any other circumstance that Camerafirma deems must be considered to this respect shall be published on Camerfirma's website http://www.camerfirma.com/certificados/ or upon request from the Camerfirma Support Department at https://secure.camerfirma.com/incidencias/ or by telephone 902 361 207.

2.5.3 Prices for accessing 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 on Camerfirma's website http://www.camerfirma.com/area-de-usuario/consulta-de-certificados/.

Camerfirma currently offers the OCSP service free-of-charge but reserves the right to invoice these services. If invoiced, the prices of these services are published at http://www.camerfirma.com/servicios/respondedor-ocsp/.

2.5.4 Prices for accessing the content of these Certification Policies.

Accessing the content of this CPS is free-of-charge on the Camerfirma website https://policy.camerfirma.com.

2.5.5 Refund policy.

AC Camerfirma does not have a specific refund policy, and adheres to general current regulations.

2.6. Publication and repositories.

2.6.1 Publication of CA information.

In general, Camerfirma publishes the following information in its repository:

- An up-to-date directory for certificates in the repository that indicate the certificates issued and whether they are valid or whether their validity has been cancelled or is expired.
- The lists of revoked certificates and other information about the revocation status of certificates.
- The general certification policy and, when it is deemed convenient, the specific policies.
- The profiles of the certificates and the revocation lists for the certificates.
- The Certification Practice Statement.
- The legally binding instruments with subscribers and verifiers.

All amendments made to the service specifications or conditions are communicated to users by the Certification Entity, through the website http://www.camerfirma.com

The previous changed version of the document will not be removed; it will be indicated that it has been replaced by the new version.

Certificates are published by external SubCAs in a repository provided by AC Camerfirma, or if applicable, in their own repository, by means of a contractual agreement, which Camerfirma shall have access to.

2.6.1.1 Certification Policies and Practices.

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

The SubCAs certification policies are also published or referred to AC Camerfirma's website.

2.6.1.2 Terms and conditions.

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

2.6.1.3 Distribution of the certificates.

The issued certificates can be accessed as long ***as the Signatories/Subscribers give their consent***. Prior to issuing the certificate, the applicant undertakes an acceptance of the uses, granting Camerfirma the rights to publish the issued 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 web site by entering the subscriber's email address. If a subscriber with that email address is found, the system displays a page with all the related certificates, whether active, expired or revoked. This consultation service is therefore not free-of-charge, and the mass download of certificates is prohibited.

2.6.2 Publication frequency.

AC Camerfirma **publishes the final entity certificates** immediately after they have been issued, provided that the Signatory/Subscriber has given his/her approval.

AC Camerfirma frequently issues and publishes lists of revocation documents following the table indicated in the section of this practice document **"Issuing frequency of CRLs"**

Camerfirma immediately publishes on its website https://policy.camerfirma.com. Any modification made in the **Policies and the CPS**, keeping a record of versions.

The Camerfirma information is published when it is available and in particular, immediately published when the mentions are issued referring to the certificate validity.

The changes in the CPS are governed by the corresponding section of the CPS.

The certificate status revocation information is published pursuant to the corresponding section of this CPS.

Fifteen (15) days after publishing the new version, the reference to the change can be removed from the main page and inserted in the depository. The old versions of the documentation are conserved for a period of **fifteen (15) years** by the Certification Entity, and are available to be consulted by the interested parties should they have a valid reason to do so.

2.6.3 Access controls for the repositories.

Camerfirma publishes certificates and CRLs on its web site. The certificate holder's e-mail address is required to access the certificate directory, and an anti-robot control must be passed to therefore 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, in such a way that:

- The authenticity of the certificates can be checked. The certificate itself signed by the certification authority guarantees its authenticity.
- Unauthorised persons cannot change the information. The certification authority's electronic signature protects the information included in the certificate from being tampered with.
- The certificates can only be accessed by people indicated by the signatory. The applicant authorises or rejects the publication of its certificate in the application process.
- Any technical change that affects the security requirements can be detected. The database that acts as a repository is equipped with protection mechanisms for data integrity and unauthorised access.

2.7. Audits.

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 subjecting its certification system, and fundamentally the RAs, to internal audits every two years, in order to ensure compliance with internal procedures.

Camerfirma is subject to regular audits with the **WEBTRUST for CA, WEBTRUST SSL BR and WEBTRUST SSL EV** seal, which guarantees that the policy documents and CPS have the appropriate format and scope and are fully aligned with their certification policies and practice.

Camerfirma is also subject to the controls that the national regulatory agency undertakes with regards to its activity, which is the Ministry for Industry of the Government of Spain.

The Registration Authorities belonging to both hierarchies are subject to an internal audit process. These audits are frequently carried out in a discretionary manner based on a risk assessment for the number of certificates issued and the number of registration operators, which also determines whether the audit is carried out on-site or remotely. The audit processes are described in an "Annual Audit Plan".

AC Camerfirma is subject to an audit process every two years complying with the LOPD.

AC Camerfirma carries out an audit process for entities that have obtained a SubCA or TSU certificate and which issues and manages certificates with its own technical and operational resources.

2.7.1 Audit frequencies

As indicated in section 2.7, Camerfirma carries out an approved audit process each year, in addition to the internal audits that it carries out in a discretionary manner.

- Audit ISO 27001, ISO20000, WEBTRUST for CA, WEBTRUST SSL BR, WEBTRUST SSL EV every year.
- Twice-yearly LOPD audit.
- RA audits in a discretionary manner.
- Annual external TSU SubCA audits.

2.7.2 Auditor identification and rating

The audits are carried out by independent, external companies that are widely renowned in IT security, IT system security and audit processes, in compliance with the Certification Authorities:

- For the WEBTRUST Auren audit.
  http://www.auren.com.
- For the ISO27001/20000 AENOR audits.
  http://www.aenor.es/aenor/inicio/home/home.asp
- For the internal /RA/SubCA, TSA Auren LOPD audits
  http://www.auren.com/

2.7.3 Relationship between the auditor and the CA

The audit companies used are independent and reputed companies with specialist IT audit departments in the management of digital certificates and reliable services, which rules out any conflict of interest that could affect their work with the CA.

2.7.4 Topics covered in the audit

In general lines, 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 suitably manages the security of its information systems.
e) In the OV and EV certificates, the audit process checks the alignment with the policies established by CA/B FORUM both in the "Baseline Requirement" and the "EV SSL Certificate guidelines".

In general lines, the elements subject to audit are the following:

- Processes undertaken by Camerfirma, RAs and elements related to the issuing of time stamp, TSA and OCSP online validation service certificates.
- IT systems.
- Protection of the data process centre.
- Documentation required for each type of certificate.
- Verification that the RA operators know the CPS and AC Camerfirma Policies.

2.7.5 External SubCA audits.

AC Camerfirma, through its auditors, undertakes an annual audit process for the organisations that have obtained a SubCA or TSA certificate and which issue certificates with their own technical and operational resources. This audit process can be replaced by a favourable WebTrust audit certificate for CA and/or WebTrust for EV as the case may be for the certificates issued.

2.7.6 Auditing the Registration Authorities

Every RA is audited. These audit processes are carried out at least every two years in a discretionary manner and based on a risk assessment. These audits check the compliance with the Certification Policy requirements in relation to the undertaking of registration duties established in the signed service agreement.

As part of the internal audit, samples are taken of the issued certificates to check that they have been processed correctly.

Reference documentation with respect to the audit processes of the RA is:

IN-2010-04-12-RA Security Evaluation Procedure
IN-2010-04-15-Record of the Evaluation Visit
IN-2010-04-16-Check List
IN-2006-03-08-RA Duties Procedure.
IN-2010-04-17-Evaluation Report

2.7.7 Audit report handling

Once the audit has been carried out and the report received, Camerfirma shall discuss the shortcomings found with the entity that completed the audit and develop and execute a corrective plan to resolve these shortcomings.

If the Entity audited is not able to develop and/or execute the corrective plan requested, or if the shortcomings found represent an immediate threat to the security or integrity of the system, communication must be sent immediately to the Policies Authority, which may execute the following actions:

- Temporarily cease operations.
- Revoke the corresponding certificate, and regenerate the infrastructure.
- Terminate the service offered to the Entity.
- Other complementary actions as deemed necessary.

2.8. Confidentiality

2.8.1 Type of information to be kept confidential

Camerfirma considers any information not classified as public to be confidential. Information declared confidential is not distributed without express written consent from the entity or organisation that classified it as confidential, unless established by law.

Camerfirma has established a policy for processing information and forms that anyone accessing confidential information must sign.

Reference documentation:

IN-2005-02-04-Security Policy.
IN-2006-02-03-Security Regulations.

Camerfirma strictly complies with data protection law. This document is valid as a security document pursuant to Law 59/2003 on Digital Signatures.

Reference documentation:

IN-2006-05-11-Compliance with legal requirements

2.8.2 Type of information considered not confidential

Camerfirma considers the following information not confidential:

a) The content of this CPS and the Certification Policies.
b) The information contained in the certificates.
c) Any information whose publishing is prohibited by applicable law or regulations.

2.8.3 Distribution of information on certificate revocation/suspension

Camerfirma distributes information on the suspension or revocation of a certificate by publishing it regularly on the CRLs.

Camerfirma provides a CRL and Certificate consultation service on the following website: http://www.camerfirma.com/area-de-usuario/consulta-de-certificados/

The policy for disseminating certificate revocation information in External SubCAs with the use of their own technology shall be carried out based on their own CPC.

2.8.4 Sending information to the Competent Authority

Camerfirma provides the information that the competent authority or the corresponding regulatory agency requests, in compliance with current law.

2.9. Intellectual property rights

Camerfirma owns the intellectual property rights for this CPS. The property of the CPS of the SubCAs related to the Camerfirma hierarchies belongs to Camerfirma, without prejudice to transfers of their rights in favour of the SubCAs and without prejudice to the contributions of the SubCAs themselves that belong to them.

3. Identification and Authentication

3.1. Initial registration

3.1.1 Types of names

The Signatory/Subscriber is described in the certificates 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 documents. Similarly, it includes a "Common Name" component (CN =).

The syntactic structure and the content of the fields of each certificate issued by Camerfirma, as well as its semantic meaning, shall be described in each one of the certificate profile documents.

- In certificates corresponding to **natural persons** the identification of the signatory is formed by their name and surname(s), in addition to their tax identification code.
- Certificates corresponding to **legal entities** shall be identified by means of their corporate or business name and tax identification code.
- The **final entity certificates that describe machines or services** include an identification name for the machine or service, additionally the legal entity that owns the said service in the organisation field "O" of the "CN".
- The structure for the **SubCA, 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 identification number of the organisation responsible for the keys (SN)
  - The country where the corporate activity of the organisation responsible for the keys is undertaken. (C)
- The **Secure Server** certificate includes, depending on the type of FQDN domain certificate (Fully Qualified Domain Name) for which the organisation "O" described in the company has ownership and control.
- The **ROOT** certificates have a descriptive name that identifies the Certification Authority and in the field (O) the name of the organisation responsible for the Certification Authority.

3.1.2 Pseudonyms

The acceptance or not of pseudonyms is dealt with in each certification policy. If accepted, Camerfirma uses the Pseudonym with the CN attribute of the Signatory/Subscriber's name, keeping the Signatory/Subscriber's real identity confidential.

The pseudonym in certificates in which it is allowed is calculated in such a way that it unmistakeably identifies the real certificate holder, **attaching an organisation's acronym to the certificate serial number.**

3.1.3 Rules used to interpret several name formats

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

3.1.4 Uniqueness of names

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

3.1.4.1 Issuing several natural person certificates for the same owner.

Under this CPS a subscriber can apply for more than one certificate, provided that the combination of the following values existing in the application are different for a valid certificate:

Tax identification code Corporate tax identification code
National tax identification code Tax identification code for natural person
Type of certificate (Certificate description field).

As an exception, this CPS allows a certificate to be issued when the Corporate Tax identification code, National tax identification code, Type, all coincide with an active certificate, provided that another differentiating element exists between them, in the fields TITLE and/or DEPARTMENT.

3.1.5 Name dispute settlement procedure

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

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

Camerfirma complies with section 2.4.4 of this CPS.

3.1.6 Recognition, authentication and function of registered trademarks

Camerfirma does not assume any obligations regarding the issue of certificates in relation to the use of a trademark. Camerfirma does not purposefully allow the use of a name for which the Signatory/Subscriber does not own the right to use. Nevertheless, Camerfirma is not obliged to search for proof of ownership of trademarks for issuing certificates.

3.1.7 Methods of proving private key ownership.

Camerfirma uses various circuits 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 Policies.

a) Keys created by Camerfirma (KPSC)

   These are given to the subscriber in person or by mail via protected files, using Standard **PKCS#12**. The security of the process is guaranteed due to the access code of the document **PKCS#12** enabling the installation of this code in the applications, it is delivered by means of a different channel to the one used for receiving the document (e-mail, telephone).

   Camerfirma can give keys to the Signatory/Subscriber directly or via a registration authority on a security card (DSCF).

b) Keys created by subscriber. (KUSU)

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

3.1.8 Authentication of the identity of an individual, the entity and their relationship.

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

To correctly identify the identity of the Applicant, the entity and their relationship, Camerfirma establishes the following requirements through the RA:

3.1.8.1 In the RA operator certificates.

On the one hand, it is checked that the applicant has passed the operator exam and on the other hand, that the information is identical to that in the RA operator document delivered by the organisation to which the operator belongs. It is checked that the Tax identification code is associated with the organisation and that the e-mail associated with the certificate is an e-mail of the organisation.

3.1.8.2 In recognised certificates.

Those that are described in such a way under the Signature Law 59/2003, as well as the Electronic Access Law for Citizens to Public Services 11/2007.

3.1.8.2.1 Identification of the Applicant.

The Signatories/Subscribers are required to appear in person when they are also the Applicant, or the Applicant's representative when this is a legal entity, and they as well as presenting the following:

- National Identification Document.
- Residency card.
- Passport.

Within the certificate, the identification of the holder is included in the field "Serial Number" of the "CN" indicating the identification number. The type of document used is included in the "non-critical" extension of the "CN" with OID 1.6.5 1.3.6.1.4.1.17326.30.4. It may be that the certificate holder is a company with which the identification information, in this case, shall correspond to the information and documents that identify the company.

Physical attendance is not required for these certificates in the cases established in Law 59/2003.

The documentation necessary to issue a certificate is published at:

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

3.1.8.2.2 Identification of the Entity.

Prior to the issuing and delivering a certificate for an organisation, the information must be authenticated with regards to the formation and legal nature of the entity. 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 web site.

Documentation proving that the public administration, public body or public entity exists is not required, because the said identity forms part of corporate scope of the General State Administration or other State Public Administrations.

The documentation necessary to issue a certificate is published at:

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

Within the certificate, the identification of the company associated with the certificate holder is included in the "non-critical" extension of the "CN" with OID 1.6.5 1.3.6.1.4.1.17326.30.2, and the type of supporting document in the “non-critical" extension of the “CN” with OID 1.6.5 1.3.6.1.4.1.17326.30.3.

In the certificate profile documents it can be seen in which field the identification document number is included and, if applicable, the type of document.

The profile documents can be requested through the AC Camerfirma customer support service 902 361 207 or through the application https://secure.camerfirma.com/incidencias.

3.1.8.2.3 Identification of the relationship.

For the **Special Power of Attorney Certificate and Power of Representation Certificate**, the notary deeds must be submitted to prove the Signatory/Subscriber's powers of representation in relation to the entity. A certificate issued by the public register at least **10 days** previously is submitted. The RA can also check the status and level of the applicant's powers of representation online.

In the Special Powers of Representation Certificates, the different powers are described in a table of sections, which are included in the certificate in two ways: one, placing the sections of the powers of representation in the TITLE field, and two, by means of a link in the USER NOTICE that forwards the deeds that have been scanned and signed by the RA operator. The list of powers of attorney can be found at:
https://www.camerfirma.com/apoderado/poderes.php.

For the **Relationship certificates**, usually a signed authorisation from a legal representative or proxy must be submitted.

In the **Legal entity certificates**, where the Signatory/Subscriber and the Applicant are different, documentary evidence is required that the Applicant has sufficient powers to apply for the certificate on behalf of the Signatory/Subscriber, in the form of a certificate from the public registry issued in the last **10 days** or by the RA making an online query of the corresponding public record.

In the **Public Employee/Headquarters and Seal Certificates** the identification document of the person who is acting as responsible for it, on behalf of the said Public Administration, Agency or Public Law

Entity. The Applicant/person responsible is identified by the RA with his/her National Identification Document and the authorisation of the person responsible, where it is indicated that he/she is a public employee or appointed in the Official Bulletin where the person's National Tax Identification code appears.

3.1.8.3 For technical or component certificates.

3.1.8.3.1 For OV (Organisation Validation) secure server certificates.

In order to validate an application for an OV (Organisation Validation) secure server certificate the following is checked:

1. **The entity's existence** by accessing public registers (www.registradores.org; www.rmc.es), Camerdata (www.camerdata.es), Informa (www.informa.es) or the databases of the Spanish Tax Agency (www.aeat.es). The entity is described in the Organisation field of the certificate and matches the domain owner. The circumstances may arise in which a certificate is issued for this type of self-employed person, in this case, an entity does not exist, which is identified by means of an up-to-date receipt from the IAE tax in addition to their Identification Document.
   For entities outside of Spanish territory, the documentation that must be provided is the Official Registry of the corresponding country, duly apostilled, where the existence of the entity in the said country is indicated.

2. **The existence of the domain or ID address** and the subscriber's right to use it. This is checked by accessing the WHOIS Internet domains. The use of a domain name or private IP addresses is allowed but is obsolete (and will be prohibited after October 2016, meaning that Camerfirma will stop issuing certificates of this kind from **1 November 2015**. In any case, issued certificates of this type are revoked if their expiry date is later than **October 2015**. The customer will be 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 corresponding ccTLD or gTLD shall be applied.

3. **The subscriber's control over the domain**, checking that the information found in the WHOIS Internet service search matches the entity's information submitted in the application.

   It may occur that the domain is assigned in the registrar's database to a third parry responsible for its management. In such circumstances, in order for the last domain owner's details to appear in the certificate, the following is needed:

   a. An authorisation of this for issuing the certificate.
   b. Communication indicating these circumstances from the organisation or person that controls the domain record.

The certificate is delivered via email to at least the administrative and technical supervisors who appear in the domain databases. The STATUS management application does not allow the validation of certificates without entering the administrative and technical contact details, which are automatically notified.

In the certificates issued with a SAN extension (SubjectAltName). The aforementioned procedures must be executed for each of the domains included in the certificate. The certificate cannot be issued if any of them do not comply with the indicated requirements.

Camerfirma check the record of the authorized issuer CAA, according to RFC 6844. Camerfirma only issue a Web certificate if CAA entry in the DNS Record have a value “camerfirma.com” o is empty.

3.1.8.3.2 In the corporate digital seal certificates.

The issuing of the **corporate digital seal certificates** is supported with documents in the following way: an enquiry into the existence of the company/entity is checked in the AEAT, Camerdata, Informa or public registry databases, in the same way as for the issuing of the aforementioned OV secure server certificates. The applicant's email address must come from an account with a domain related to the company or body that made the application.

The certificate is downloaded from the STATUS management platform by the applicant, for which they have previously received an e-mail with the downloading instructions. The document with the key information and the certificate is subsequently downloaded. An e-mail is then received with the information required in order to install the keys.

To complete the procedure, authorisation from the subscriber is requested, which can be issued by a legal or human resources department.

3.1.8.3.3 In code signing certificates.

For **code signing certificates,** the same checking system is used as for the issuing of OV secure server certificates.

3.1.8.3.4 In encryption certificates.

The **encryption certificates** are issued online, using a valid, recognised certificate in the process.

Pursuant to this CPS, encryption certificates can be issued in batch processes. In this case, the identity can be checked via remote processes, submitting a document with the applicant's identity and relationship with the entity to an RA or to Camerfirma. This remote process is only used when the certificate is for exclusive encryption use.

3.1.8.3.5 In EV secure server certificates.

For *"extended validation"* **Secure Server Certificates (EV)** that follow the *"CA/Browser Forum Guidelines for Issuance and Management of extended validation certificates"*, the same procedures apply as for a Recognised contractual relationship certificate, i.e.:

1. The Signatories/Subscribers, or an Applicant's representative if it is an entity, must introduce themselves in person and present an identity document or passport. In the event of entities outside of the Spanish territory, the passport of specific, duly apostilled document attesting to the country must be presented.
2. The RA requests the required documentation depending on the type of entity in order to identify it. The entity's business activity must be proven. This is checked by accessing the commercial registry or other business activity registers. In the event of entities outside of the Spanish territory, the documentation that must be provided is the Official Registry of the corresponding country, duly apostilled, where the existence of the entity in the said country appears.
3. Submission of authorisation signed by an entity's representative, who acts as the Applicant. In the event of entities outside of the Spanish territory, the documentary accreditation for the representation powers of the person signing the authorisation must be provided, duly apostilled, in order to check the authenticity of the documentation provided.

For these certificates, the RA must also check:

1. The entity's existence:

   By accessing public registrars (www.registradores.org; www.rmc.es), (www.registradores.org; www.rmc.es), Camerdata (www.camerdata.es), Informa (www.informa.es) or the databases if the Spanish Tax Agency (www.aeat.es). If the RA operators require further information on the organisation than appears on the certificate, they can access a corporate risk management database **Camerfirma SA https://www.camerfirma.com**. This database provides commercial registry information on companies and their representatives, including risk information. In the event of entities outside of the Spanish territory, the documentation that must be provided is the Official Registry of the corresponding country, duly apostilled, where the existence of the entity in the said country appears.

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

2. The existence of the domain and the subscriber's right to use it is checked by accessing the WHOIS domain databases:
   - http://www.internic.net/whois.html
   - http://www.networksolutions.com
   - http://en.gandi.net
   - http://www.interdomain.es
   - https://www.nic.es/ (.es)
   - http://www.eurid.eu/ (.eu)
   - http://www.nic.coop/whoissearch.aspx (.coop)
   - http://www.nominalia.com/
   - http://www.arsys.es/

3. That the entity has control over the Internet domain for which the certificate has been issued. In other words, the entity described in the internet domain database access service is clearly identified and matches the entity that the certificate applicant is representing.

The certificate issue guidelines require that a distinction 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 the information is accurate. The certificate includes this information as defined in the reference certification policies.

In the certificates issued with the SAN extension (Subject Alternative Name). The aforementioned procedures must be executed for each of the domains included in the certificate. The certificate cannot be issued if any of them do not comply with the indicated requirements.

3.1.8.3.6 In the SubCA, TSU certificates.

For the issuing of a SubCA or TSU certificate, a service agreement is previously signed with the applicant, having recognised their existence, their legal representatives and their powers for the distribution of the certificates under the AC Camerfirma hierarchy. This decision is made by the company's senior management.

3.1.8.4 User identification considerations in cases of senior management.

AC Camerfirma uses special procedures for identifying senior management in companies and administrations for issuing digital certificates. In these circumstances, a record operator visits the organisation's premises in order to guarantee the physical presence of the owner. For the relationships between the owner and the organisation represented in public administration, the publication of roles in the official bulletins is normally used.

3.1.8.5 Considerations in the user identification and relationship in the AAPP.

There are aspects to be considered with regard to the record authorities established in the public administration and operated by public employees, the latter are considered notaries in order to guarantee the relationship between a public employee who applies for the certificate and the agency with which he/she is associated. In these circumstances, the collection of documentation that forms part of the record can be simplified.

3.1.8.6 Special considerations for issuing certificates outside of Spanish territory.

Aspects that are related to the identification documentation for natural persons, legal entities and relationships between them in the different countries where Camerfirma issues certificates. The documentation required for such purposes is that which is established by law in each country, provided that it allows compliance with the corresponding identification obligation pursuant to Spanish legislation.

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

3.2. Key renewal

Before renewing a certificate, Camerfirma checks that the information used to verify the identity and other such information of the subscriber and key owner is still valid.

In certificates on which renewal is allowed, the owner is authenticated based on the certificate to be renewed.

Under this practice, if any information about the subscriber or owner of the key has changed, a new certificate must be registered and issued, pursuant to the corresponding sections in this document.

Camerfirma always issues new keys to renew certificates. The technical process is therefore the same as the one followed to make a new application.

When **qualified or recognised certificates** for electronic signatures are renewed, the Law for Electronic Signatures 59/2003 allows the issuing of certificates without physical presence for a period of up to **five years** from the last on-site registration. Once the period established has transpired, the subscriber must follow the same on-site issue process as for the first issue. Under these practices, if more than five years have not passed at the time of the certificate renewal, the physical presence of the owner is not required.

STATUS, the management application used by Camerfirma makes four notifications (30 days, 15 days, 7 days, 1 day) by e-mail to the subscriber advising that the certificate is going to expire.

The renewal process can be initiated on the Camerfirma website http://www.camerfirma.com/area-de-usuario/renovacion-de-certificados/. This process requires a valid certificate (not revoked) which is to be renewed.

- Once the certificate being renewed has been identified, the application presents the subscriber the old certificate details and requests confirmation. The application allows the subscriber 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 application is included in the RA application. Once the operator has checked the information, they proceed with issuing the certificate to the CA.

- As a general rule, Camerfirma issues a new certificate taking the expiry date of the certificate being renewed as the start date for the new certificate. In some circumstances, in web services issue processes, the certificate can be renewed with the date at the time of renewal, and the former certificate being renewed will subsequently be revoked.

Technical certificates (secure server, corporate seal and code signing) cannot be renewed; a new certificate must always be issued by starting a new application process.

SubCA certificates are not automatically renewed; they must be issued in a new process based on prior planning, controlling that the valid duration of the certificate is always greater than the maximum validity duration of the certificates that are issued under its hierarchical line.

RA Operator certificates are renewed every year, provided that there is no knowledge that the certificate holder is no longer an RA Operator.

TSU certificates are issued with a duration of six years and a private key use of one year, meaning that they are renewed on a yearly basis.

ROOT certificates. ROOT certificates are issued in a new process by means of a ceremony held for such a purpose.

OCSP certificates are frequently issued and renewal processes are not established.

3.3. Re-issue following a renewal

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

Exception:

> When final entity certificates are revoked as a result of a **replacement** process for the certificate or as a result of an error **or loss** in its issue, it is considered that it can be renewed after a revocation provided that it reflects the current situation. The supporting document submitted for the issuing of the replacement certificate is re- used and the on-site appearance, if required due to the nature of the certificate, is eliminated. Camerfirma updates the number of years since the last physical appearance to the status of the certificate being replaced, just as if this process were the result of an ordinary renewal.

3.4. Certificate renewal without key renewal

AC Camerfirma does not allow certificate renewal without key renewal.

3.5. Certificate renewal with key renewal

Since this is the common process for renewing AC Camerfirma certificates, the processes described in this section refer to this renewal method.

3.6. Changes to certificates

Any need to change certificates shall involve a new application. The certificate is revoked and a new certificate issued with the correct information.

In the case of a certificate replacement process, it is considered a renewal and the renewal years are thus calculated without physical appearance as established by law.

Changes can be made to certificates, such as renewals, when the attributes of the subscriber or the owner of keys that form part of the control of uniqueness set forth for this policy have not changed.

If the changes are applied for within an ordinary period provided for within the certificate renewal, the certificate is renewed instead of making changes and revoking the certificate to be changed.

3.7. Application for renewal

The method for requesting revocation is established in section 4.5.

4. Operational requirements

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

4.1. Certificate application

4.1.1 Online forms.

Certificates are usually applied for by accessing the application forms at the address, or by sending the applicant a link to a specific form.

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

The web site contains the forms required to apply for each type of certificate that Camerfirma distributes in different format and the signature creation devices, if necessary.

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

The user receives an e-mail, after confirmation of the application data, at the address associated with the certificate application, with a link to confirm the application and accept the conditions of use.

Once the application has been confirmed, the subscriber is informed of the documentation that must be presented at an authorised registration office and that he/she must comply with the physical attendance identification requirements, if applicable.

SubCA, TSA certificates must be applied for through the application for a commercial offer and subsequently included in the STATUS platform application forms.

4.1.2 Batches.

The STATUS platform also allows application circuits using batches. In this case, the applicant sends the RA a file structured according to a design pre-established by Camerfirma containing the applicants' details. The RA uploads these applications into the management application.

4.1.3 Final entity certificate application in HSM, TSU and SubCA.

Applications for issuing certificates in HSM, TSU or SubCA must be made through a commercial offer application through a local sales agent. http://www.camerfirma.com/camerfirma/localizacion.

AC Camerfirma reserves the right to send an internal or external auditor to check that the key creation ceremony conforms with certification policies and corresponding practices.

When the customer creates the his/her own encryption keys in an HSM device and requests a hardware certificate, Camerfirma compiles the necessary evidence, for which the following documentation is requested:

- Statement of compliance from the applicant indicating that the keys have been created within a hardware device and/or a technical report from a third party (service provider) that certifies this process. AC Camerfirma provides statement models for subscribers and third parties.

- Minutes of the key creation ceremony indicating:

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

- Characteristics of the device: A technical document for the device may be suitable

This information is included on behalf of the RA in the supporting documentary record for issuing the certificate.

For each type of certificate, the subscriber must accept the terms and conditions of use between the subscriber, 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 web site before creating and downloading the certificate.

4.1.4 Applications through a Web Services (WS) layer.

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

The "blind" issuing of this type of certificate means that the process is revised in detail. Before starting to issue certificates using this system, a favourable Camerfirma technical report must be available, an agreement in which the registration authority is obliged to maintain the system in optimal security conditions and to notify Camerfirma of any changes or incidents. The system must also be subject to annual audits in which the following aspects are checked:

1. Documentary records for the certificates issued
2. That the certificates are being issued under the guidelines established by the certification policies under which they are governed.

4.1.5 Certification application procedure

Once a certificate application has been submitted, the RA operator verifies the information provided by accessing the management platform (STATUS), pursuant to the corresponding section of this DPC.

The operator of the STATUS platform has an internal management certificate that is issued in order to carry out these operations and which is obtained after a training and evaluation process.

The registration operator looks at the pending applications requiring processing based on a distribution of projects. In other words, the operator only sees the applications that enter a project to which he/she is associated.

The RA operator waits for the subscriber to present the corresponding documentation.

If the information is not correct, the RA denies the application. If the information is correctly verified, the Registration Entity approves the issue of the certificate by means of the electronic signature with its RA operator certificates.

Applications made through web services are directly executed when they are received and authenticated with a certificate that has previously been recognised by Camerfirma.

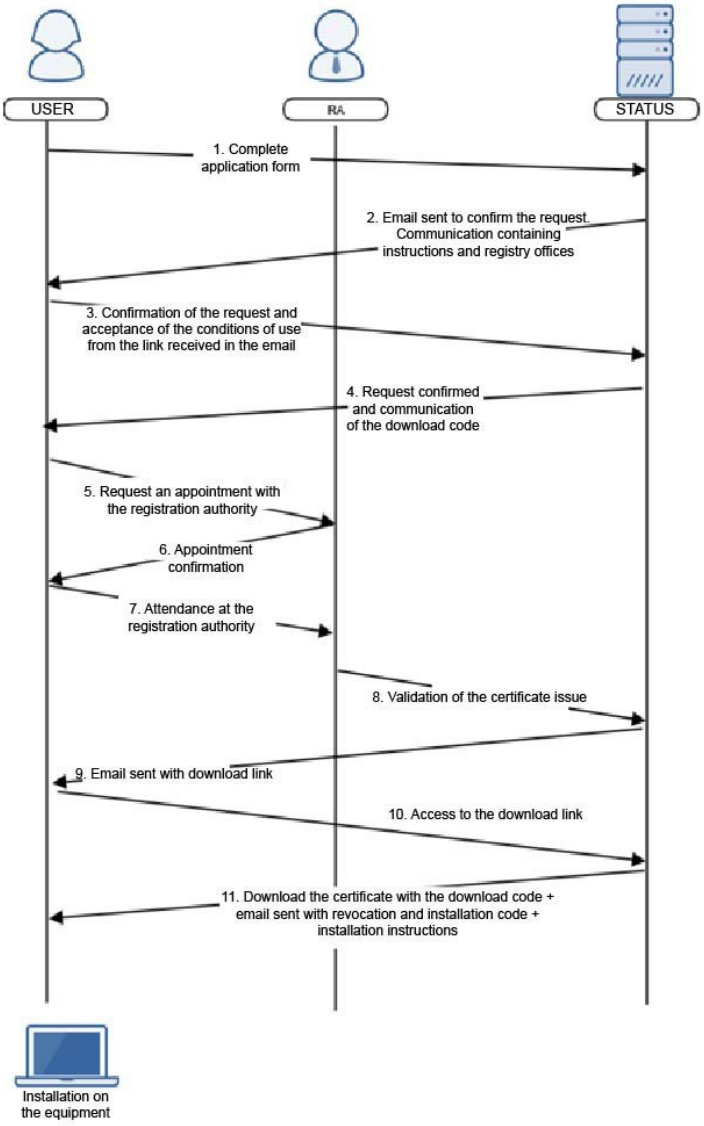
4.2. Cross certification application.

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

4.3. Certificate issue

4.3.1 Certificates via Software:

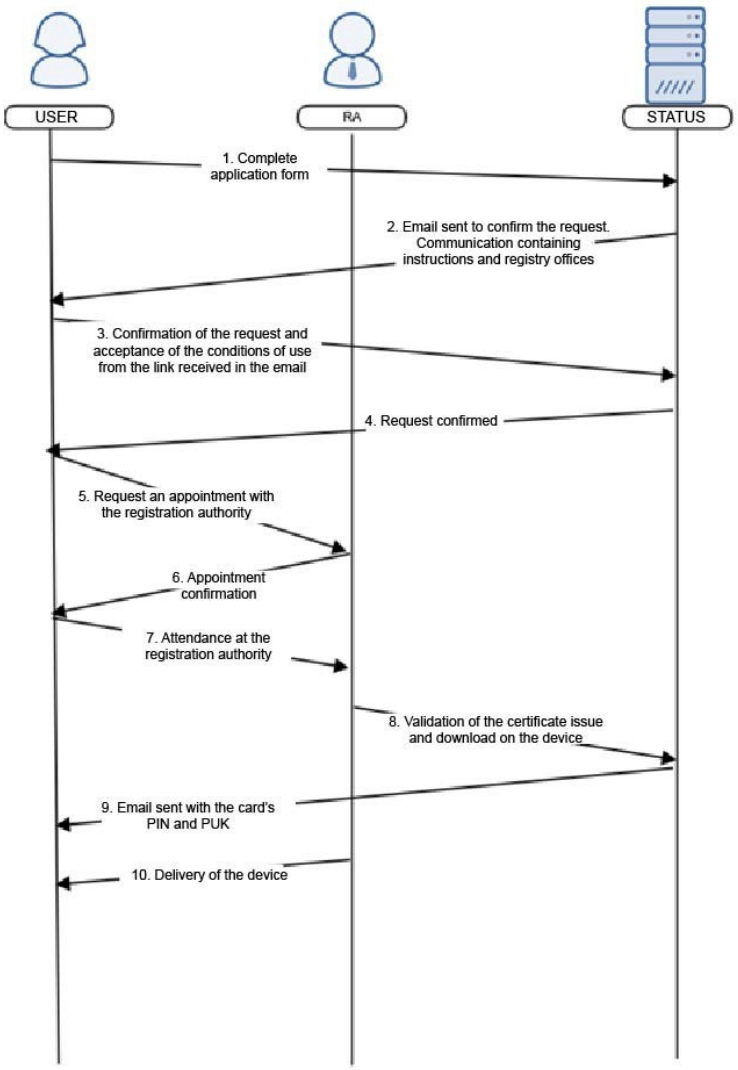
Once the application has been approved, the subscriber receives an e-mail with the approval notification, from which the certificate can be created and downloaded. The product code provided with the contract and an installation code sent in a separate email or via SMS together with a revocation code is required to install it.



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

4.3.2 Certificates in HW (Secure Signature Creation Device):

4.3.2.1 Cryptographic Card or Token:



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

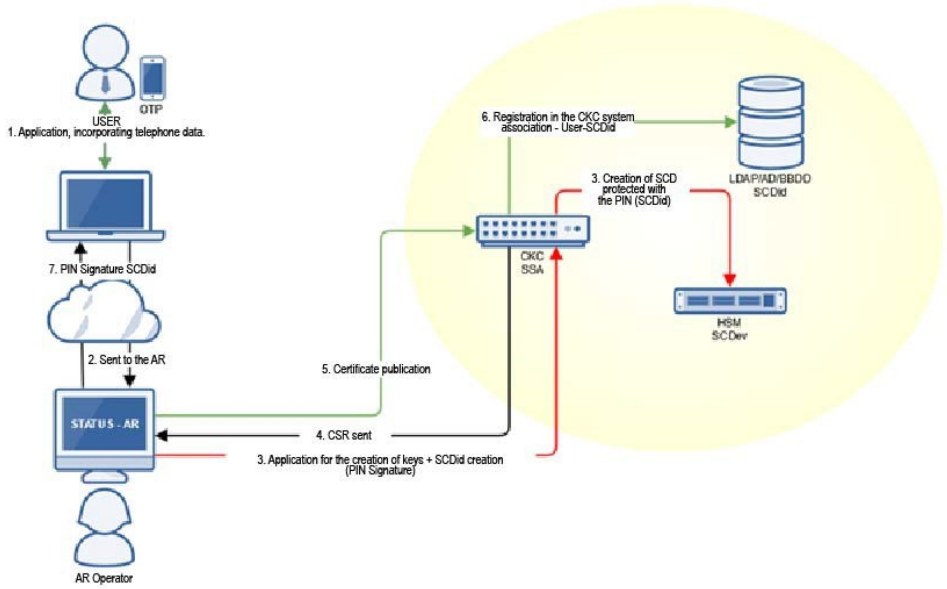
The Registration Authority operator chooses which cryptographic card to use to create the keys. For this purpose, the operator's work station is suitably configured with the corresponding CSP (Cryptographic Service Provider). AC Camerfirma currently allows several types of USB cards and tokens, all CWA 14169 SSCD Type-3 certified.

For the default cards (distributed by bit4id) the subscriber receives an e-mail in the associated account containing the access code to the cryptographic device

and the unlocking code, as well as a renewal key. For other cards, the PIN/PUK management is outside of the scope of this document.

Reference document: **IN-2008-03-02**-Generacion_certs_tarjeta_tecnico

4.3.2.2 Certificates on centralised key management platform.



AC Camerfirma has a solution for the centralised key management system. The keys are created in an HSM FIPS 140 2 level three where they are stored for subsequent use by the public key certificate holders that are associated with them.

On the STATUS platform, the Registration Authority operator chooses to create the keys on a centralised cryptographic device. The operator's work station must therefore be configured with the CSP (Cryptographic Service Provider) corresponding with the centralised key creation device.

Subscribers must have client software installed on their PC in order to allow their local key store to be linked securely to the real keys stored on the centralised PC.

The subscribers receive the private key activation codes by email. This means they have exclusive control of the key.

At this time, the centralised key management system is awaiting recognition by the Ministry for Industry as a secure signature creation device.

4.3.2.3 Applications via WS: Applications can be received via duly signed calls to the STATUS application WS services layer, pursuant to section 4.1.4.

4.3.3 EV secure server certificates

Pursuant to the specific policies for **EV secure server certificates**, these certificates require the physical presence of the applicant or an approved third party. The RA manager verifies the service payment, the related documentation and the Signatory/Subscriber's identity.

The certification policies for issuing SSL EV certificates, to which this DPC adheres ("CA/Browser Forum Guidelines for Issuance and Management of extended validation certificates"), require that each EV certificate issue application 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 operations department checks the documentation and definitively validates and issues the certificate.

Subscribers can use their own resources to create the keys in a cryptographic device and deliver the application to Camerfirma in PKCS10 format to issue the certificate. In the event that the certificate is issued with a hardware format with an HSM device, evidence is requested to verify this, for example as described in point 4.1.3. of this document.

If the private key is created by Camerfirma, once the RA operator has approved the application, the following is sent to the Signatory/Subscriber:

- ✓ A link to the web page where the certificate is created in PKCS#12 format.
- ✓ A password required to install the keys and the certificate on the signatory's computer.
- ✓ The Signatory/Subscriber also requires a downloading code for the key and certificate creation process, which is supplied by the application in the application process.

If the key is created by the subscriber, Camerfirma sends a certificate to the user in PKCS#7 format.

4.3.4 Encryption certificate.

Encryption certificates are also issued automatically once the holder has submitted a valid identity document to the web application developed for that purpose, at

http://www.camerfirma.com/certificados/compontentes/certificado-camerfirma-cifrado/

or via certificate batch applications, based on which Camerfirma issues PKCS#12 files.

AC Camerfirma stores a copy of the keys and the certificate in software format PKCS#12, maintained secure by a password distributed between 4 AC Camerfirma operators. At least two of them must participate in order to recover the decryption key.

4.3.5 SubCA applications:

SubCA certificates are issued in a SubCA certificate issuing ceremony at AC Camerfirma's premises in a safe environment and under the supervision of an auditor.

4.4. Certificate acceptance.

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

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

4.5. Notification of the issue to interested parties

Camerfirma notifies the applicant by e-mail of the approval or rejection of the application.

4.6. Publication of the certificate

The issued certificates are published at this link http://www.camerfirma.com/area-de-usuario/consulta-de-certificados/

AC Camerfirma uses its STATUS® platform to publish certificates and CRLs at the customer's offices in such a way that the information can be accessed locally. It can be published in an active directory, an LDAP service or a database.

4.7. Notification of the issue to third parties

AC Camerfirma offers an enquiry system for the status of the issued certificates, on their website http://www.camerfirma.com/area-de-usuario/consulta-de-certificados/. Access to this web page is free.

In some cases, it is a requirement of the national supervisor that the certificates and CRL issued by the provider are periodically sent.

In the event of SSL EV certificates, a notification is sent before issuing the certificate to different accredited registration services. This requirement is of obligatory compliance for the acknowledgement of SSL EV certificates by Google in a process called "Certificate Transparency".

4.8. Certificate suspension and revocation.

4.8.1 Preliminary clarifications

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), in other words, a certificate is revoked temporarily until it is decided whether it should be revoked definitively or activated.

Rendering an electronic 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 consultation service (publication of a list of revoked certificates or consultation in 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 their validity expires, they are removed from the list of revoked certificates. Camerfirma only eliminates a certificate from the revocation list in either of the following situations:

- Certificate expired
- Certificate revoked due to suspension, and once reviewed there are no reasons found to justify it being revoked definitively.

4.8.2 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 is revoked where:

- Any of the details contained in the certificate are amended.
- Errors are detected in the data submitted in the certificate application or there are changes to the verified circumstances for the issue of the certificate.
- Failure to receive payment 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 subscriber or certificate manager is compromised or suspected of being compromised.
- There is unauthorised third party access or use of the subscriber's or certificate manager's private key.
- There is misuse of the certificate by the subscriber or certificate manager, or failure to keep the private key safe.

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 subscriber's or certificate manager's activation details.

Due to circumstances affecting the subscriber or certificate manager.

- The relationship is terminated between the Certification Authority and the subscriber or certificate manager.
- There are changes to or termination of the underlying legal relationship or cause for the issue of the certificate to the subscriber or certificate manager.
- The applicant breaches part of the requirements established for applying for the certificate.
- The subscriber or certificate manager breach part of their obligations, responsibility and guarantees established in the legal document or in this Certification Practices Statement.
- The sudden disability or death of the subscriber or certificate manager.

- The certificate's subscribing legal entity is terminated, thus finalizing the subscriber's authorization for the person responsible for the certificate, or the relationship between the subscriber and person responsible for the certificate is terminated.
- The subscriber requests revocation of the certificate pursuant to the provisions of this CPS.
- 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, pursuant to the relevant section of this CSP.

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

- If the certificate holder or natural person applicant requests the revocation of an individual certificate, they must present a signed statement that indicates the certificate to be revoked and the reason for the application and identify themselves before the RA.

- If the revocation is requested on behalf of a third party, an authorisation must be presented either from the natural person certificate holder or the legal representative of the natural person certificate holder, which indicates the reasons for which the certificate revocation is requested and identify themselves before the RA.

- If the Entity associated with the certificate holder requests the revocation due to the termination of the relationship, these circumstances must be accredited (revocation of powers, contract termination, etc.) and the certificate holder must identify him/herself before the RA as having sufficient powers to represent to the Entity.

Subscribers have revocation codes that can be used in the online revocation services or by calling the help lines.

4.8.3 Who can request revocation?

Certificate revocation can be requested by:

- The Signatory/Subscriber

- The responsible Applicant

- The Entity (via a representative)

- The RA or CA.

Camerfirma can, in case you locate an error in the certificate, revoke it unilaterally within a maximum period of 1 week. Depending on the severity and in case the user's security may be compromised, the provider may unilaterally revoke the certificate within 24 hours.

Anyone established in the specific certification policies.

4.8.4 Revocation request procedure.

All requests must be made:

Via the online Revocation Service, by accessing the revocation service on the Camerfirma web site 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 and presenting the Signatory/Subscriber or Applicant's **National Identification Document.**
- ✓ By sending Camerfirma a document signed by a representative with sufficient representative capacity for the Entity, requesting the certificate revocation. This method is used for the revocation of SubCA and TSU certificates.
- ✓ For **secure server, corporate seal or code sign certificates**, this revocation can be requested by e-mail, using the address used to request issue of the certificate, sending the revocation request to gestión_soporte@camerfirma.com. The Camerfirma operator will confirm the request by telephone in order to process it.

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

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

Both **the revocation management service and the consultation service are considered critical services, as specified in Camerfirma's contingency plan and business continuity plan.** These services are available 24 hours a day, 7 days a week. In the event of a system failure, or any other circumstance out of Camerfirma's control, Camerfirma will make every effort to ensure the services are not down for more than a maximum period of **24 hours.**

In the event of a revocation due to the failure to pay the fee for the issued certificate, the RA or the CA will previously request, and on two successive occasions, at the contact e- mail address, that the subscriber rectifies this situation within a period of eight days. Failure to do so will result in immediate revocation of the certificate.

4.8.5 Revocation period

The revocation period, from the moment Camerfirma or an RA has reliable knowledge of a certificate revocation, happens immediately, and is included in the next CRL issued as well as in the database of the management platform, which supplies the OCSP respondent.

4.8.6 Suspension

When a certificate is suspended, Camerfirma has **one week** to decide on the certificate's definitive status: (revoked or active). If the information required to verify and validate the revocation request is not provided within this period, Camerfirma will revoke the certificate definitively.

If the certificate is suspended, notification is sent to the Signatory/Subscriber by email specifying the time of suspension and the reason.

If the certificate is not suspended and has to be activated again, the Signatory/Subscriber will receive an email specifying the new certificate status.

The suspension process is not applied to the certificates

- TSU
- AC
- RA Operator.

Procedure for the suspension request
The suspension can be requested on the corresponding page of the Camerfirma website or by contacting Camerfirma by phone, in person or by previously authenticated written communication. The subscriber must have the revocation code in order to proceed with the certificate suspension.

4.8.7 Suspension period limits

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

Camerfirma will supervise, via a certificate management platform alert system, that the suspension period established by the Policies and this CPS is not exceeded.

4.8.8 CRL issue frequency

AC	Issued every...	Duration
CHAMBERS OF COMMERCE ROOT	**365 days**	**365 days**
CAMERFIRMA CHAMBER OF COMMERCE CERTIFICATES	24 hours	48 hours
CAMERFIRMA PUBLIC ADMINISTRATIONS	24 hours	48 hours
CAMERFIRMA EXPRESS CORPORATE SERVER v3	24 hours	48 hours
CAMERFIRMA CODESIGN v2	24 hours	48 hours
CAMERFIRMA TSA	24 hours	48 hours

CHAMBERSIGN ROOT	**365 days**	**365 days**
AC CAMERFIRMA	365 days	365 days
RACER	24 hours	48 hours

CHAMBERS OF COMMERCE ROOT – XXXX	**365 days**	**365 days**
CAMERFIRMA CHAMBER OF COMMERCE CERTIFICATES – XXXX	24 hours	48 hours
CAMERFIRMA PUBIC ADMINISTRATION – XXXX	24 hours	48 hours
CAMERFIRMA CORPORATE SERVER – XXXX	24 hours	48 hours
CAMERFIRMA CODESIGN – XXXX	24 hours	48 hours
CAMERFIRMA TSA – XXXX	24 hours	48 hours

GLOBAL CHAMBERSIGN ROOT – XXXX	**365 days**	**365 days**
AC CAMERFIRMA – XXXX	365 days	365 days
RACER – XXXX	24 hours	48 hours
AC CAMERFIRMA COLOMBIA – XXXX	365 days	365 days
AC CITISEG – XXXX	24 hours	48 hours
GOVERNMENT OF ANDORRA	24 hours	48 hours
CGCOM	24 hours	48 hours

4.8.9 CRL checking requirements

Trusting third parties must first check the status of the certificates before their use, , and in any case must check the latest CRL that has been issued, which can be downloaded from the following website:

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

Camerfirma always issues CRLs signed by the CA that issued the certificate. The access to the CRL is also referred to in the certificate extension "CRL distribution points".

4.8.10 Availability of online service to check revocation

CA provides an online service to check revocations via HTTP at:

http://www.camerfirma.com/area-de-usuario/consulta-de-certificados/
Also by means of OCSP queries at:

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

The addresses for accessing these services are included in the digital certificate. For the CRL and ARL 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 based on CRLs issued by the various certification authorities (CAs) or by access to the database of the platform (EE). The 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 a day, seven days a week**, **365 days a year.**

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

4.8.11 Requirements of the online service to check revocation

To check a revocation, the Trusting Third Party must know the e-mail address related to the certificate to be consulted if it is accessed online.

The requirements to access the **OCSP** service and the certificates required to validate it are updated at:

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

4.8.12 Other methods of distributing revocation information

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

4.8.13 Checking requirements for other methods of distributing revocation information

Not stipulated

4.8.14 Special revocation requirements due to compromised key security

Not stipulated

4.9. Security Control Procedures

Camerfirma is subject to the annual validations established by the UNE-ISO/IEC 27001:2007 standard, which regulates the establishment of suitable processes to ensure correct security management in information systems.

4.9.1 Types of recorded events

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

The following events are recorded:

- ✓ System start-up and shut-down.
- ✓ Creation, deletion and setting up of passwords or changed privileges.
- ✓ Attempts to log in and out.
- ✓ Unauthorised access attempts to CA's system online.
- ✓ Unauthorised access attempts to file system.
- ✓ Physical access to logs.
- ✓ Changes to system settings and maintenance.
- ✓ CA application logs.
- ✓ CA application switching on and off.
- ✓ Changes to the CA's details and/or its 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 life cycle of the cryptographic module, like its receipt, use and uninstallation.

Camerfirma also conserves, whether manually or electronically, the following information:

- The key creation ceremony and the key management databases.
- Physical access records.
- Maintenance on and changes to the system configuration.
- Personnel changes.
- Obligation and discrepancy reports.
- Material destruction records that contain key information, details of the activation or the subscriber's personal information, in the case of individual certificates, or the key owner, in the event of an organisation's certificates.

- Owning activation information, for operations with the private key of the Certification Entity.
- Complete reports for physical intrusion attempts in the infrastructures that offer support to the issuing and management of certificates.

4.9.2 Log processing frequency

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

The processing of the auditing records consists of a revision of the records that includes the verification that they have not been tampered with, a brief inspection of all of the record entries and a more detailed investigation into any alert or irregularity identified in the records. The actions carried out following the auditing revision are documented.

Camerfirma maintains a system that guarantees:

- Sufficient space to store logs
- That the log files are not overwritten.
- That the information that is saved includes, at least: event type, date and time, user executing the event and result of the operation.
- The log files are saved in structured files that can be included in a database for data mining later on.

4.9.3 Storage periods for audit logs

Camerfirma stores the log data for at least **five years**.

4.9.4 Protecting audit logs

The system logs are protected from being manipulated via signatures in the files that contain them.

They are stored in fireproof devices.

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

The log files can only be accessed by authorised persons.

The devices are always handled by authorised personnel.

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

4.9.5 Audit log backup procedures

Camerfirma uses a suitable backup system to ensure that, in the event important files are lost or destroyed, the 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 log on an external device once a week.

A copy is also kept at an external custody centre.

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

4.9.6 Audit data collection system

The information from the auditing of events is collected internally and automatically by the operating system, the network and by the certificate management software, in addition to by the manually created information, which is stored by duly authorised personnel, all of which forms the auditing record accumulation system.

4.9.7 Notifying the party that caused the event

When the auditing record accumulation system records an event, there is no need to send the individual, organisation, device or application a notification indicating what caused the event.

A communication can be sent to advise whether the action was successful or not, but not that the action has been audited.

4.9.8 Analysing vulnerability

The analysis of vulnerabilities is covered by the Camerfirma audit processes. The risk and vulnerability management processes are reviewed once a year in accordance with the scope of the review of the certification UNE-ISO/IEC 27001:2007 that appear in the document Risk Analysis with code **CONF-2005-05-01**. This document specifies the controls implemented to guarantee the required security objectives.

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

4.10. Record files

4.10.1 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
- ✓ All the information related to certificates, including contracts with signatories and RAs. The information related to their identification and location.
- ✓ Applications to issue and revoke certificates.
- ✓ Type of document presented in the certificate application.
- ✓ Identity of the Registration Entity that accepts the certification 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 archiving all of this material.

4.10.2 File storage period

The certificates, contracts with the Signatories/Subscribers and any information related to the identification and authentication of the Signatory/Subscriber are kept for at least **15 years**.

The old versions of the documentation are also kept for a period of 15 (fifteen) years by AC Camerfirma, and can be consulted for any justified reason by the interested parties.

4.10.3 File protection

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

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

4.10.4 File backup procedures

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

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

Camerfirma, as a minimum, makes daily, progressive back-up copies of all of its electronic documents and makes complete, weekly back-up copies for cases involving information recovery.

4.10.5 Requirements for log time stamping

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

Camerfirma has a software security document that describes the time and date settings of the parameters for the systems used in the issuing of certificates.

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

4.10.6 Audit data collection system

Camerfirma has a centralised data collection system for activity on devices involved in the certificate management service.

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

4.10.7 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 back-up procedure

4.11. Changing the key

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

In CA (Root CA, SubCA) :

Before the CA certificate expires, a change of key will be made. The certificate to be updated by the CA and its private key is only used for the signing of CRLs while active certificates exist issued by this CA. A new CA certificate is created with a new private key and a CN (*common name*) that is different to the CA certificate to be replaced.

A CA certificate is also changed when the status of the cryptographic type (algorithms, size of keys, etc.) requires it.

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

4.12. Retrieval in the event of compromised key security or natural disaster

Camerfirma has developed a contingency plan to retrieve critical systems, if an alternative data centre were necessary, as part of the UNE-ISO/IEC 27001:2007 certification.

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

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

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

4.12.1 An entity's key is compromised

The Camerfirma contingency plan set forth in the UNE-ISO/IEC 27001:2007 certification covers compromised CA private keys and disaster situations.

If the security of a root key is compromised:

- All the Signatories/Subscribers, Trusting Third Parties and other CAs with which agreements or other relationships regarding a breach of security have been established are informed.
- They are informed that the certificates and information relating to the revocation status that are signed using this key are not valid.

4.12.2 Security installation following a natural or other type of disaster

Camerfirma will re-establish the critical services (revocation and publication of revoked certificates) pursuant to the contingency and business continuity plan set forth in the UNE-ISO/IEC 27001:2007 certification indicating re-establishment in the following 24 hours.

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

4.13. Termination of CA activity

Before the CA ceases its activity, Camerfirma will:

- Provide the required funds (via a public liability insurance policy) to complete the revocation processes.
- Inform all the Signatories/Subscribers, Trusting Third 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 issue procedure.
- Pass on its obligations related to keeping log data for the established time period to the subscribers and users.
- The CA's private keys are destroyed or disabled.
- Camerfirma will keep any activate certificates and the verification and revocation system until all the issued certificates have expired.

5. Physical, Procedural and Personnel Security Controls

Camerfirma is subject to the annual validations established by the UNE-ISO/IEC 27001:2007 standard, which regulates the establishment of suitable processes to ensure proper security management in information systems.

5.1. Physical Security Controls

Camerfirma has established physical and environmental security controls to protect resources in the buildings where the systems and equipment used for the operations 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 **24/365** assistance and assistance during the **24 hours** following the notification.

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.

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

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 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, CPD 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.

The cryptographic devices, and mediums that store keys from the Certification Entities, have a specific system and additional to the rest of the building, for the protection against fire.

5.1.6 Storage systems

Each dismountable 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 of use, it is destroyed using suitable means for the device containing it.

Handouts and paper: using paper shredders or waste bins provided for such a purpose, later destroyed using controlled means.

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

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

5.1.8 External back-up

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 remove devices.

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

5.2. Procedural controls

5.2.1 Roles of trust

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

In order the determine the sensitivity of the function, the following elements are taken into account:

- Duties associated with the function.
- Level of access.

- Monitoring of the function.
- 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 incompatible with Systems. These duties are subordinated to Operations Management, reporting to this Management and to the Technical Department.

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

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

RA Administrator:
Responsible for approving certification applications from the subscriber.

Security Manager:
Responsible for coordinating, controlling and complying with the security measures defined by the Camerfirma security policies. The security manager is be responsible for aspects 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 the tasks described in the Certification Policies, Mainly handling the Root CA and intermediate CA key storage device.

5.2.3 Identification and authentication for each role

The people assigned to each role are identified by the internal auditor who must ensure that each person carries out the procedures to which he/she is assigned.

Each person only controls the assets that are 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 Switching the PKI management system on and off

The PKI system is made up of the following modules:

RA Management Module, for which the specific page manager services is activated or deactivated.

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

Application Management Module, for which the specific page manager services are activated or deactivated.

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

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

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

TSA module. Time stamp 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 system 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 in the production centre for at least **one year** and have a permanent employment contract.

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

The personnel working in positions of trust are not found to have personal interests that come into conflict with the performance of the role that they are appointed.

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 application validation duties.

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

Camerfirma will not assign a trusted or management role to a person who is not suitable for the position, especially if he/she has been convicted for theft or if there is any doubt about their suitability for the position. For this reason, an investigation is previously carried out, to the extent that applicable legislation allows it, in relation to the following aspects:

- Studies, including alleged qualifications.
- Previous work experience, up to five years, including professional references and checking that they did actually perform the alleged role.
- Delinquency

Reference documentation:

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

IN-2005-02-17-Human Resources 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 the necessary investigations before hiring anyone.

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

In the application for the role they are informed of the need to be subject to a prior investigation and they are warned that the refusal to be subject to the investigation will result in the rejection of the application. Similarly, unequivocal consent from the affected party for the prior investigation and processing and protection of all of the personal information pursuant to the data protection law.

5.3.3 Training requirements

Personnel undertaking duties of trust must have been trained pursuant to the Certification Policies. There is a training plan that is part of the UNE-ISO/IEC 27001:2007 controls.

Registration operators who validate EV secure server certificates receive specific training pursuant to the special regulations on the issue of these certificates.

The training includes the following content:

- Security principles and mechanisms of the public hierarchy of certification.
- Hardware versions and applications in use.
- Tasks that the person must undertake.
- Management and processing of security incidents and obligations.
- Business continuity and emergency procedures.
- Management and security procedure in relation to the management of personal information.

5.3.4 Information updating requirements and frequency

Camerfirma undertakes the required updating procedures to ensure certification duties are undertaken correctly, 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 previously 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 carried out in this section, or in other parts of the CPS, apply to and are complied with by the third party undertaking the duties of the operation of certification services, the certification entity being held responsible at all times for the proper execution.

These aspects are specified in the legal instrument used to agree on the provision of certification services by a third party other than Camerfirma; the third parties are obliged to meet the requirements established by Camerfirma.

Reference documentation: **IN-2006-05-02**-Provisions applicable to external developers

5.3.8 Documentation given to personnel

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

Any documentation that employees require is also supplied at all times so that they can perform their duties competently.

6. Technical Security Controls

6.1. Key pair creation and installation

6.1.1 Creating the key pair

The systems used by Camerfirma are nCipher. These devices house root keys and are certified **Level 3 FIPS 140-2**.

The root keys are created and managed in a offline system in a cryptographic room. Reference document CONF-00-2012-02-CA creation script root 2008

SubCA keys are created in HSM systems, where they are housed for their corresponding use. The certificate issued by the root key is created in a secure cryptographic room.

CA Certificate	Length of the key	Algorithm of the signature *1	Start date	Expiry date
Chambers of Commerce Root	**2048**	**1**	**2003**	**30/09/2037**
AC Camerfirma Chamber of Commerce Certificates	2048	1	2004	09/02/2034
AC Camerfirma Codesign v2	2048	1	2009	18/01/2019
AC Camerfirma Express Corporate Server v3	2048	1	2009	18/01/2019
AC Camerfirma TSA CA	2048	1	2005	20/05/2035
Global Chambersign Root	**2048**	**1**	**2003**	**30/09/2037**
AC Camerfirma	2048	1	2003	14/11/2033
RACER	2048	1	2003	04/12/2023
Chambers of Commerce Root – 2008	**4096**	**1**	**2008**	**31/07/2038**
Camerfirma AAPP – 2012	4096	1	2012	14/07/2022
Camerfirma AAPP II – 2014	4096	2	2014	15/12/2037
Camerfirma Chamber of Commerce Certificates – 2009	4096	1	2009	14/03/2019
Camerfirma Codesign – 2009	4096	1	2009	14/03/2019
Camerfirma Codesign II – 2014	4096	2	2014	15/12/2037
Camerfirma Corporate Server – 2009	4096	1	2009	14/03/2019
Camerfirma Corporate Server II – 2014	4096	2	2014	15/12/2037
Camerfirma TSA – 2009	4096	1	2009	14/03/2019
Camerfirma TSA – 2013	4096	1	2013	19/02/2037
Camerfirma TSA II – 2014	4096	2	2014	15/12/2037

Global Chambersign Root -2008	4096	1	2008	31/07/2038
AC Camerfirma – 2009	4096	1	2009	11/03/2029
RACER – 2009	4096	1	2009	23/03/2019
OMC	4096	1	2014	21/11/2024
Entitat de Certificació de l'Administració Pública Andorrana	4096	1	2013	13/07/2033
AC Camerfirma Colombia – 2014	4096	1	2014	27/09/2036
AC CITISEG – 2014	4096	1	2014	26/09/2036

*1 SHA1WithRSAEncryption = 1
SHA256WithRSAEncryption = 2

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

Reference documentation:

CONF-00-2012-01 **MINUTES 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 subscriber's key pair

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

If the certificate is qualified and requires a secure signature creation device; it is only used with these devices to make electronic signatures.

The management platform creates a random, strong password with its own resources, and a protected private key, with the said password, using the 3DES algorithm. Based on this private key, a certificate signature application is created in the PKCS#10 format. With this application, the CA makes the subscriber's certificate signature. The certificate is delivered to the user in a PKCS#12 document in which the certificate and the private key associated with it are included. The password of the private key and the PKCS#12 document is never clear in the system.

The keys are created using the algorithm of the **RSA** public key.

The keys can also be created in a remote RA system using the WEB services layer for the PKCS10 application and the corresponding collection of the PKCS7.

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

Notes on the centralised key management system:

If a centralised key management system is implemented, a storage device is always used for the user keys, which must comply with at least **FIPS-140-2 level 3 and guarantee the unique control of the key by double factor authentication.** Depending on whether the device that stores the keys and manages its use is certified and recognised by the corresponding national regulatory agency as a secure device for creating signatures based on applicable technical legislation, the signature produced is considered, recognised/qualified, advanced or simple.

6.1.2 Delivering the public key to the certificate issuer

The public key is given to Camerfirma to create the certificate when the circuit requires in a standard format, preferably self-signed **PKCS#10** or **X509** format.

6.1.3 Delivering the CA public key to users

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

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

6.1.4 Size and validity of issuer's keys

See section 6.1.1

6.1.5 Size and validity of subscriber's keys

The Signatory/Subscriber'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 subscriber certificates is encrypted pursuant to RFC 3280 and PKCS#1. The algorithm for creating keys is the RSA.

6.1.7 Checking parameter quality

Size of keys = minimum 2048 bits.
Key creation algorithm: rsagen1
Padding scheme: emsa-pkcs1-v1_5
Hash functions: SHA-1 / SHA-256

6.1.8 Key creation hardware/software

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

The **ROOT 2008** keys have used a cryptographic device. nShield PCI 500 F3 by nCipher. This device complies with the specifications **FIPS 140-2 level two and level three**.

6.1.9 Purpose of key use

The keys are only used for the purposes indicated in the section "Purpose of key use" of the certification policies of each one of the certificates issued.

The CA makes every possible effort that is in within their scope to confirm that the CA signature keys are only used for certificate creation purposes and for the signing of CRLs.

Despite the fact that the encryption of information is technically possible with the certificates, Camerfirma shall not be held responsible for the damages caused due to the holder's loss of control of the private key needed to decipher the information, except in the certificate exclusively issued for this use. For certificates that are not exclusively for encryption, Camerfirma does not copy or store private keys associated with them.

6.2. Protecting the private key

The CA's private key

The Root signature private key and the CAs are kept in an nCipher cryptographic device. This device complies with the specifications **FIPS 140-2 level 3.**

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

The external SubCA keys are kept in devices that comply with at least FIPS 140-1 level 3.

The subscriber's private key

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

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

As regards cryptographic devices with certificates for advanced electronic signing, suitable as secure signature creation devices, these comply with security level CC EAL4+ and support the PKCS#11 and CSP standards.

Camerfirma uses the cryptographic means allowed in its registration application and which guarantee the creation of recognised electronic signatures.

Information on the type of key creation and safekeeping is included in the digital certificate itself, allowing the Trusting Third Party to act accordingly.

Notes on the centralised key management system:

If a centralised key management system is implemented, a storage device is used for the user keys, which must comply with at least FIPS-140-2 level 3. The key is activated remotely by means of a personal and secret key sent to the certificate holder or the person responsible for the keys from the management platform, guaranteeing the unique control of the private key on their behalf.

6.3. Standards for cryptographic modules

See 6.2

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

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

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

6.3.2 Custody of the private key

Camerfirma does not store or copy the subscriber's private keys when they are created by the PSC and they are subject to the electronic signature law 59/2003. For certificates on hardware devices it is the user who generates and keeps the private key in the cryptographic card delivered by the PSC.

Camerfirma only stores a copy of the subscriber's private key when this is "exclusively" used for information encryption purposes or those certificates associated with the keys that are not subject to the electronic signature law 59/2003.

Notes on the centralised key management system:

This document considers the responsibility of the organisation that houses the users' private keys, in a centralised key management system.

Camerfirma stores these keys in an experimental mode in the distribution of certificates with centralised keys, taking i the new European regulation in which this practice is permitted into account. In this system, the user keys are stored and protected by a certified cryptographic device FIPS 140-2 level 3.

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

Camerfirma keeps minutes on CA private key management processes.

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

6.3.4 Archiving the private key

ACS private keys are archived 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 private key from the initial cryptographic device.

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

Subscribers can only store the private key for as long as they deem appropriate in the case of encryption certificates. In this case, Camerfirma also keeps a copy of the private key linked to the encryption certificate.

Camerfirma keeps minutes on CA private key management processes.

6.3.5 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 **MINUTES from key creation events.**

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

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

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

Keys linked to subscribers cannot be transferred.

Camerfirma keeps minutes on CA private key management processes.

Notes on the centralised key management system:

If a centralised key management system is implemented, the system generates the user keys on a centralised cryptographic device.

6.3.6 Private key activation method

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

The Root key is activated by means of 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 minutes on CA private key management processes.

Notes on the centralised key management system:

If a centralised signing system is implemented, subscribers receive a unique, secret activation password, which allows them to activate the private key remotely in the same way as a local key store. Before activating the key, the user must have authenticated the centralised management application where the user identity is associated with the key stored in the centralised device.

6.3.7 Private key deactivation method

For the certificates on card, the subscriber's private key is deactivated once the cryptographic device used to create the signature is taken out of 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 entity, CA, SubCA, TSU keys, a cryptographic ceremony is performed for which the corresponding minutes are created.

The keys in the centralised cryptographic device, as well as their possible copies, are deactivated by deletion following the corresponding device manuals.

6.3.8 Private key destruction method

Before the keys are destroyed, a revocation of the certificate of the associated public keys 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 subscriber's keys stored on software can be destroyed by deleting them in accordance with instructions from the application on which they are stored.

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

Camerfirma keeps minutes on CA private key management processes.

Reference document: **IN-2006-05-01**-Destroying User Keys

6.4. Other aspects of managing key pairs

6.4.1 Filing the public key

Pursuant to article 20 f) of Law 59/2003 on Electronic Signatures, the CA conserves its files for a minimum period of **fifteen (15) years** provided that technology at the time allows this. The documentation to be kept includes public key certificates issued to subscribers and proprietary public key certificates.

6.4.2 Period of use for public and private keys.

A public or private key certificate must not be used once its validity period has expired.

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

6.5. Activation data

6.5.1 Creation and activation of activation data

The CA activation data is created and stored in cryptographic smart cards that are only kept by authorised personnel.

6.5.2 Protection of activation data

Only authorised personnel know the PINs and passwords to access the activation data.

6.5.3 Other aspects of activation data

Not stipulated.

6.6. Secure signature creation device life cycle.

The CA certificates of the **Chamber of Commerce Root or Global Chambersign Root** hierarchies store the subscriber's keys in a secure signature creation device **(hardware)** or in a secure storage device for signature creation information **(software)** with this situation being reflected in the content of the certificate itself.

The **software** device is delivered in **PKCS#12** format for import into the applications. The file is kept in the subscriber's custody for retrieval. The installation data must be kept separately from the key file.

Another case of software devices is the use in secure server certificates where the keys are created with the page server application resources.

The **hardware** device is a cryptographic card or USB token that complies with accreditation requirements established under current law or at least **ITSEC E4+.** These devices are described on Camerfirma's website http://www.bit4id.com/es/descargas_camerfirma_bit4id.htm

As regards hardware devices

a) Hardware devices are prepared and stamped by an external provider.
b) The external provider distributes the device to the registration authorities to be delivered to the subscriber.
c) The subscriber 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 subscriber or RA, which is entered into the device.
e) The device can be reused and can store several key pairs securely.

6.7. 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 electronic certification systems.

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

The computers used are initially configured with the appropriate security profiles by Camerfirma system personnel:

1. Operating system security settings.
2. Application security settings.
3. Correct system dimensioning.
4. User and permission settings.
5. Log event settings.
6. Backup and retrieval plan.
7. Anti-virus settings.
8. Network traffic requirements

6.7.1 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
- ✓ subscriber'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 via a combination of operating system, KPI software, physical protection and procedures.

6.7.2 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.

6.8. Life cycle security controls

6.8.1 System development controls

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

Reference documentation:

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

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

6.8.2 Security management controls

6.8.2.1 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 in this regard.

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

6.8.2.2 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-Classification and inventory of shares**

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**

6.8.2.3 Management procedures

Camerfirma has established an incident management and response procedure via an alert and periodical 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 the information classification requirements. Devices containing sensitive data are destroyed securely if they are no longer required.

Reference documentation:

CONF-2006-01-04-Device Input and Output Registration Procedure
IN-2005-02-15-Classification and inventory of assets

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-2010-10-08 Settings 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 solve them, including recording responses and an economic assessment of the incident's resolution.

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**

6.8.2.4 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, anti-virus 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 pursuant to the roles policy.

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

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

Creating the certificate

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

Revocation management

Certificates are revoked via strict card-based authentication of an authorised administrator's applications. The 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.

6.8.2.5 Managing the cryptographic hardware life cycle

Camerfirma makes sure that the cryptographic hardware used to sign certificates is not manipulated during transport, by inspecting the delivered material.

Cryptographic hardware is transported using means designed to prevent any manipulation.

Camerfirma records all of the important information contained in the device to add to the assets catalogue.

At least two trusted employees are required 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 is deleted once the device has been taken away.

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 minutes. These configurations are carried out by at least two trustworthy employees.

6.8.3 Life cycle security evaluation

Not stipulated

6.9. 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.

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

6.10. Time Sources

Camerfirma has established a time synchronisation procedure in coordination with the ROA Real Instituto y Observatorio de la Armada in San Fernando via NTP. It also obtains a reliable source via GPS and radio synchronisation.

Reference documentation: **IN-2006-04-01-Time synchronisation**

6.11. Cryptographic module engineering controls

All of the CA's cryptographic activities are carried out in modules validated by at least **FIPS 140-1 level three**.

7. Certificate Profiles and CRL

7.1. Certificate Profile

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

The profiles of these certificates can be requested by e-mail 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 independent documents that can be accessed from Camerfirma's web site. This publication method allows more stable policy and CPS versions and separates them from frequent changes to certificate profiles.

7.1.3 Algorithm object identifiers (OID)

The signature algorithm of the object identifier is

- 1.2.840.113549.1.1.5 – sha1withRSAEncryption
- 1.2.840.113549.1.1.11 – sha256WithRSAEncryption

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

7.1.4 Format of names.

The certificates must contain the information that is deemed necessary for its use, according to what is determined by the corresponding policy for the authentication, electronic signature, encryption or electronic evidence.

In general, the certificates to be used 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 information:

- Name and surname(s) of the subscriber, owner or representative, in separate fields, or with indications of the algorithm that allows automatic separation.
- Corporate name of the legal entity, if applicable.

- Corresponding identification document numbers, pursuant to applicable legislation for the subscriber, owner or representative, whether they are a natural person or a legal entity.

This regulation is not applicable to the certificates with a pseudonym, which must identify this status.

7.1.5 Name restrictions

The names contained in the certificates are restricted to 'Distinguished Names' X.500, which are unique and not ambiguous.

Additionally, name restrictions can be established in relation to the certificates and the corresponding policy for the authentication, electronic signatures, encryption or electronic evidence, provided that such restrictions are objective, provided, transparent and not discriminatory.

7.1.6 Certification Policy (OID) object identifier

Every certificate has a policy identifier pursuant to the following model:

<BASE>.X.Y.Z. For the certificates issued by Camerfirma the following BASE has been designated = 1.3.6.1.4.1.17326.

X = certificate type
Y = Hardware or Software.
Z = Creation of the PSC or subscriber key.

For OMC BASE = 1.3.6.1.4.1.26852
For Government of Andorra BASE = 2.16.20.2.1.3.1
For Colombia BASE = 1.3.6.1.4.1.17326

7.1.1 Use of the extension "Policy Constraints"

Not stipulated

7.1.2 Syntax and semantics of the policy qualifiers

Not stipulated

7.1.3 Semantic processing for the critical extension "Certificate Policy"

The extension "Certificate Policy" identifies the policy that defines the practice that Camerfirma explicitly associates with the certificate. The extension may contain a policy qualifier.

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 profile can be requested by e-mail 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.

OCSP profile. The profiles of these certificates can be requested by e-mail gestion_soporte@camerfirma.com or by telephone 902 361 207.

7.3. OCSP profile

7.3.1 Version number

The OCSP respondent certificates are version 3. These certificates are issued by each CA managed by AC Camerfirma according to the standard RFC 6960.

7.3.2 OCSP extensions

The profile of the OCSP respondent certificates can be by e-mail gestion_soporte@camerfirma.com or by telephone 902 361 207.

An up-to-date list of the OCSP certificates can be obtained from http://www.camerfirma.com/servicios/respondedor-ocsp.

8. Administration specification.

8.1. Policy authority

Camerfirma's legal area sets up the policy authority (PA) and is responsible for managing the Policies and CPS.

8.2. Procedures for specifying changes.

This CPS is amended when any significant changes are made to certificate management, for any type of certificate to which it applies. Revisions are conducted at least **once a year** in the event that changes have not been made in that time. These reviews are included in the version table at the start of the document.

8.2.1 Aspects that can be changed without the need for notice

Changes that can be made to this CPS do not require notification unless they directly affect the certificate Signatory/Subscribers' rights, in which case notice must be given any comments can be submitted to the policy management organisation within 15 days following publication of that notice.

8.2.2 Changes with notice

8.2.2.1 List of aspects

Any aspect of this CPS can be changed without notice.

8.2.2.2 Notice system

Any proposed changes to this policy are published immediately on Camerfirma's web site

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 made to this document are expressly communicated to those agencies and third party companies and organisations that issue certificates under this CPS.

8.2.2.3 Period for comments

The affected Signatories/Subscribers 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

8.2.2.4 Comment processing system

Any action taken as a result of comments is at the PA's discretion

8.3. 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/

8.4. 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 signed electronically with the of AC Camerfirma SA legal entity digital certificate.

9. Appendix I. Acronyms

CA	Certification Authority
CP	Certification Policy
CPS	*Certification Practice Statement*.
CRL	*Certificate Revocation List*
CSR	*Certificate Signing Request.*
DES	*Data Encryption Standard*
DN	*Distinguished Name*
DSA	*Digital Signature Algorithm*
FIPS	*Federal Information Processing Standard Publication*
IETF	*Internet Engineering Task Force*
ISO	*International Organization for Standardization*
ITU	*International Telecommunications Union*
LDAP	*Lightweight Directory Access Protocol*
OCSP	*Online Certificate Status Protocol*
OID	*Object Identifier*
PA	*Policy Authority.*
PIN	*Personal Identification Number*
PKI	*Public Key Infrastructure*
RA	Registration Authority
RSA	Rivest-Shimar-Adleman Type of encryption algorithm
SDSSCI	Secure Device for Storing Signature Creation Information
SHA	*Secure Hash Algorithm*

SSCD Secure Signature Creation Device

SSL *Secure Sockets Layer* Protocol designed by Netscape and converted into network standard, allows the transmission of encrypted information between an internet browser and a server.

TCP/IP *Transmission Control Protocol/Internet Protocol*. Protocol system, defined in the scope of the IEFT. The TCP protocol is used to divide the information in packages at its source, to later reassemble it at its destination. The IP protocol is responsible for suitably guiding the information towards its recipient.

10. Appendix II. Definitions

Activation Data	Private data, like PIN numbers or passwords used for the activation of the private key.
Applicant	Within the context of this certification policy, the applicant is a natural person empowered with special powers to carry out certain procedures on behalf of the entity.
Certificate	A file that associates the public key with some of the Signatory/Subscriber's identifying information and is signed by the CA.
Certification Authority	The entity responsible for issuing and managing digital certificates. It acts as a trusted third party between the Signatory/Subscriber and the Trusted Third Party, linking a specific public key with a person.
Certification policy	Group of rules that define the applicability of a certificate in a community and/or in a certain application, with security and common use requirements.
CPS	Group of practices adopted by a Certification Authority for issuing certificates in compliance with a specific certification policy.
CRL	File that contains a list of the certificates that have been revoked in a specific period of time and which is signed by the CA.
Crossed Certification	The establishing of a trusted relationship between two CAs, by means of the exchange of certificates between the two in virtue of similar levels of security.

Digital signature	The result of the transformation of a message, or any type of information, by the private key application in conjunction with certain known algorithms, in this way guaranteeing: a) that the information has not been changed (integrity) b) that the person who signs the information is who they say they are (identification) c) that the person who signs the information cannot deny having done so (does not repudiate its origin)
Entity	Within the context of these certification policies, a company or organisation of any kind that grants the applicant special powers.
OID	Unique identification number recorded under the ISO standard and referring to an object or type of specific object.
Pair of keys	Group formed by the public and private key, both related mathematically.
PKI	Group of elements, hardware, software, human resources, procedures, etc., that form a system based on the creation and management of public key certificates.
Policy Authority	Person or group of people responsible for all of the decisions related to the creation, administration, maintenance and deletion of the certification policies and CPS.
Private key	Mathematical value only known by the Signatory/Subscriber and used for creating a digital signature or data deciphering. Also known as **signature creation data.** The CA private key is used for certificate signatures and CRL signatures.
Public key	Mathematical value publicly known and used for the verification of a digital signature or data encryption. Also known as **signature verification data.**

Registration Authority	The entity responsible for managing the applications and identifying and registering the applicants of a certificate.
SDSSCI	Secure Device for Storing Signature Creation Information. Software or hardware element used to safeguard the Signatory/Subscriber's private key in such a way that only they have control of it.
Signatory/Subscriber	Within the context of this certification policy, the natural person whose public key is certified by the CA and has a valid private key to create digital signatures. In this Policy, the applicant's natural person coincides with the Signatory/Subscriber.
SSCD	*Secure Signature Creation Device*. Software or hardware element used by the Signatory/Subscriber for creating electronic signatures, in such a way that cryptographic operations are carried out inside the device and their control is solely guaranteed by the Signatory/Subscriber.
Trusted Third Party	Within the context of this certification policy, a person who voluntarily trusts the digital certificate and uses it as a means to accredit the authenticity and integrity of the signed document.