CERTIFICATE PRACTICES STATEMENT.

AC CAMERFIRMA SA

Version 3.2.5

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 will be 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 on new ROOT 2008 keys. Official's certificate in accordance with the implementation 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 issuing process, required by Mozilla. General review. Amended description of the person responsible for the certificate (point 1.4.8 and 2.1.3). Corrections to CRL issuing (point 2.6.2) Corrections to registration of CA Public Administrations (point 6.1.1) Add reference to HSM nCipher (point 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. See 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 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 which denote the country are changed 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 CABFORUM Changes to length of user passwords to 2048. New section 3.1.4.1

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 would like to explain its stance in relation to these concepts.

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

Certification Practice Statement (CPS): defined as a set of practices adopted by a Certification Authority for the issue of certificates. It usually contains detailed information on its certificate security, support, administration and issuing 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 the issue of certificates. The Certification Practice Statement defines **"how"** the security requirements established in the Policy are fulfilled.

1.2. General Overview

This document specifies the Certification Practice Statement (hereinafter, CPS) that CA Camerfirma SA (hereinafter, Camerfirma) has established for the issue of 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).
- 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 the Issuance and Management of Publicly Trusted Certificates V1
- CA/Browser Forum EV SSL Certificate Guidelines V 1.3

And on 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*.

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 specific Certification Policies 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 will be used to verify the OCSP responder's responses regarding the status of the certificates issued by these CAs. The Camerfirma OCSP service responses are signed electronically with a certificate of this type.

Camerfirma manages two hierarchical structures:

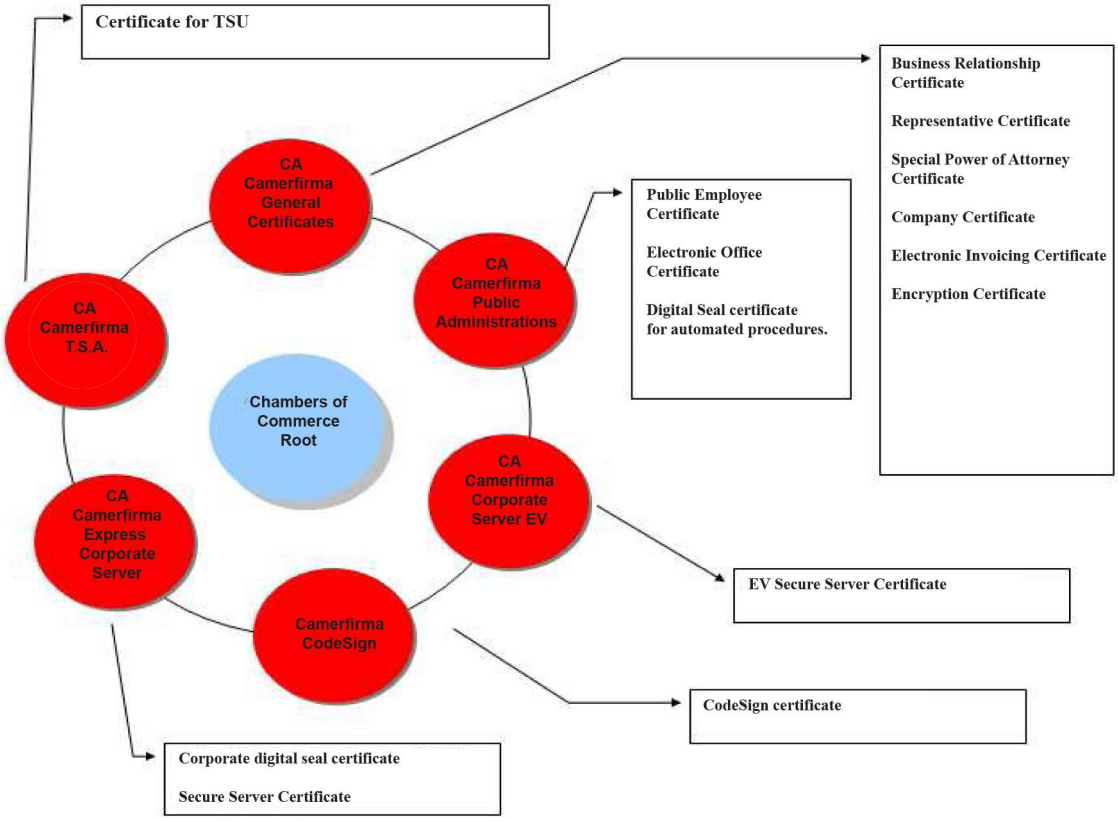
- **Chambers of Commerce Root JCC**
- **Global Chambersign Root JCS**

1.2.1.1 Chambers of Commerce Root Hierarchy (JCC) 1.3.6.1.4.1.17326.10.3.1

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.

This hierarchy includes intermediate Certification Authorities that issue digital certificates in different environments:

- **CA Express Corporate Server.** 1.3.6.1.4.1.17326.10.11.1
  - Certificates for Secure server (OV) 1.3.6.1.4.1.17326.10.11.2
  - Corporate digital seal certificate. 1.3.6.1.4.1.17326.10.11.3
- **Code Signing Authority.** 1.3.6.1.4.1.17326.10.12.1
- **Time-stamping Authority (TSA).** 1.3.6.1.4.1.17326.10.13.1
- **Camerfirma Corporate Server. (EV Secure Server)** 1.3.6.1.4.1.17326.10.14.1
- **CA Camerfirma Chamber of Commerce Certificates** 1.3.6.1.4.1.17326.10.9.1
  - 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
  - Companies. 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
- **CA Camerfirma Public Administrations** 1.3.6.1.4.1.17326.1.3.1
  - 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



1. -Express Corporate Server.
This is an intermediate CA that issues digital certificates, the owners 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 basic requirements document drafted by CA/BROWSER FORUM http://www.cabforum.org.***

- **Corporate digital seal certificate.** This certificate is related to a key stored by a machine. Procedures can be carried out automatically and without requiring intervention. The keys linked to the electronic seal certificate provide the documents and transactions to which it is applied integrity and authenticity. It can also be used as client machine identification element in SSL/TLS or HTTPS secure communication protocols, and data encryption. If a certificate is used for encryption, Camerfirma is not responsible for any resulting damages should the holder not be able to retrieve the private key required to decipher the information. For this type of certificate, Camerfirma does not copy or store private keys related to the certificate.

2. -CodeSign.
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 guaranteeing the integrity and authenticity of this code.

3. - Time stamps.
The third intermediate Authority **"AC Camerfirma TSA"** issues certificates for issuing time stamps. A time stamp is a standardised document 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 time stamp units ultimately issue the time stamps on receiving a standard request in accordance with the RFC 3161 specifications. Each of these TSUs can be associated either with the service's different technical features or exclusive client use.

CA Camerfirma issues TSU certificates to third party platforms as long as these platforms:

- Are synchronised with the time stamps established by Camerfirma
- Allow Camerfirma or an authorised third party to audit the systems.

4. - Corporate Server. EV Secure Server.
This intermediate certification authority, **"AC Camerfirma Corporate Server EV"**, issues digital certificates for Secure Server or corporate digital seals, with the same functions as the "Express Corporate Server" certification authority but subject to "CA/Browser Forum Guidelines for Issuance and Management of extended validation certificates". This regulation promotes the issuing 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 gives browsers who connect to this service an extra level of guarantee, which they can see from the green background in the browser address bar.

5. - CA Camerfirma Chamber of Commerce Certificates.
"AC Camerfirma Chamber of Commerce Certificates" is a multi-policy Certification Authority that issues qualified or recognised business relationship certifications within Spain, in accordance with 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:

Individuals with a business relationship with an Entity.

- ✓ **Contractual relationship with Entity.**
  These determine the type of contractual relationship (labour, mercantile, member of professional body, etc.) between an individual (certificate holder/signatory/subscriber) and an Entity (organisation field in certificate).
- ✓ **Powers of Representation.**
  This determines the powers of legal representation or general power of attorney between the individual (certificate holder/signatory/subscriber) and an Entity (also described in the Organisation field in the certificate).
- ✓ **Special Power of Attorney.**
  This determines the powers of specific representation or special power of attorney between the individual (certificate holder/signatory/subscriber) and an Entity (also described in the Organisation field in the certificate).

Companies.

The Company digital certificate is created in accordance with **Law 59/2003**, on Electronic Signatures, 19 December.

Camerfirma issues these certificates for any procedures arising from the relationship between the Entity (Company) and Public Administrations (tax relations, electronic invoicing, etc.) and, in general, in accordance with current law for the Company's normal business and activity, notwithstanding any quantitative or qualitative limits that may be applied.

"Camerfirma mainly issues these certificates for tax purposes, allowing companies to conduct online procedures with the Spanish Tax Office. Outside this scope, Camerfirma considers these certificates to be similar to the corporate seal and the Trusting third party must consider the signature associated with this type of certificate as such. A seal guarantees the related document's authenticity and integrity."

In the case of the Company certificate, the holder/subscriber/signatory is the Entity, although it can only be requested by one of the Entity's legal representatives or volunteers with sufficient powers for this purpose, who will act as custodian of the keys and as the party responsible for any actions undertaken with this certificate. There is the possibility, however, of assigning the keys to a third person or including them in computer software to meet each user's needs.

Electronic invoicing.

Electronic invoicing has been one of the means of promoting the use of electronic certificates. The Spanish Tax Office regulates the use of electronic certificates through Royal Decree 1496/2003. To issue an electronic invoice, an electronic document with a recognised certificate must be signed. Through the invoice certificate, Camerfirma creates a document adapted to the specific needs of electronic invoicing. The certificate is issued to an individual who the Entity expressly authorises, and its use is limited to electronic invoicing.

Encryption.

Encryption certificates are for the exclusive use of data encryption. The aforementioned certificates (relationship with entity, powers of representation, special power of attorney, electronic invoicing and company) allow the key to be used for data encryption, but Camerfirma does not keep or store the private keys belonging to the

certificate holders, in accordance with the requirements of **Law 59/2003** on Electronic Signatures, 19 December. In this situation, if the certificate holder or, in the case of the company certificate, the certificate custodian, cannot retrieve the private key, they will also lose access to all of the encrypted data with the related public key. 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 it is lost.

6.- CA Camerfirma Public Administrations

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 but also 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.

In accordance with the foregoing and the Public Administration identification and signing system, and specifically its certification policy, CA Camerfirma will issue the following types of certificates:

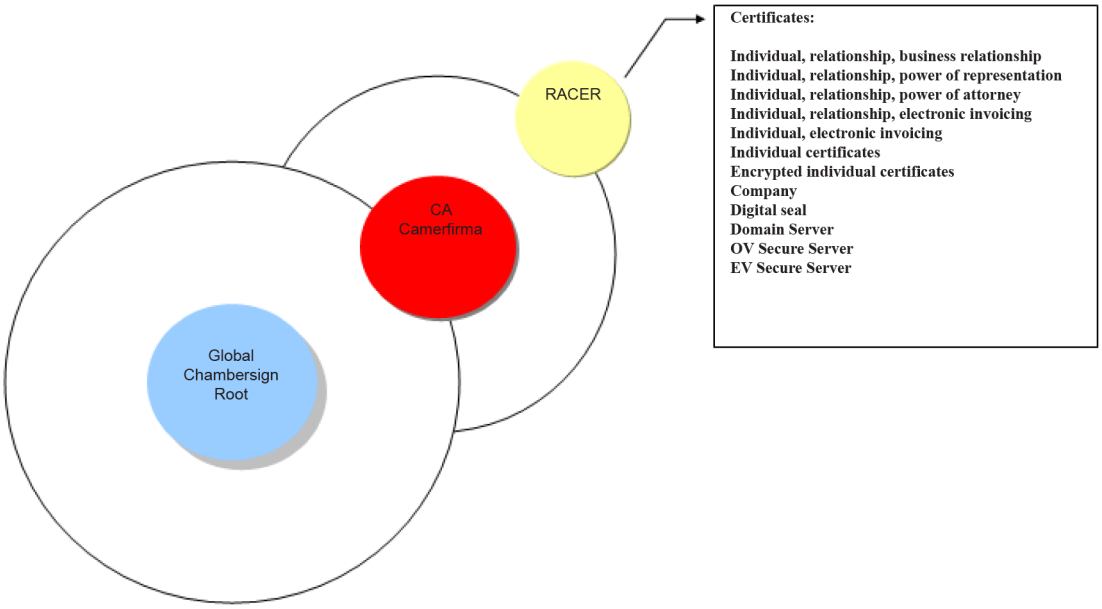
- Recognised Electronic Seal for Automated Procedures Certificate, high-level.
- Recognised Electronic Seal for Automated Procedures Certificate, high-level.
- Recognised Public Employee Certificate, high-level, signature.
- Recognised Public Employee Certificate, high-level, authentication.
- Recognised Public Employee Certificate, high-level, encryption.
- Recognised Public Employee Certificate, mid-level.
- Electronic office, mid-level.
- Electronic office, high-level.

1.2.1.2 Chambersign Global ROOT Hierarchy (JCS) 1.3.6.1.4.1.17326.10.1.1

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. Unlike the JCC, 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.

Under this hierarchy, intermediate Certification Authorities are developed:

- CA Camerfirma 1.3.6.1.4.1.17326.10.4.1
  - RACER 1.3.6.1.4.1.17326.10.8.1
    - Individual with Business Relationship, Contractual Relationship Certificate 1.3.6.1.4.1.17326.10.8.2
    - Individual with Business Relationship, Powers of Representation Certificate 1.3.6.1.4.1.17326.10.8.3
    - Company certificate 1.3.6.1.4.1.17326.10.8.4
    - Electronic seal certificate 1.3.6.1.4.1.17326.10.8.5
    - Individual Certificate 1.3.6.1.4.1.17326.10.8.6
    - Individual with Business Relationship, Electronic Invoicing Certificate. 1.3.6.1.4.1.17326.10.8.7
    - Individual with Business Relationship, Power of Attorney Certificate 1.3.6.1.4.1.17326.10.8.8
    - Individual Encryption Certificate 1.3.6.1.4.1.17326.10.8.9



1. - CA Camerfirma

The purpose of this intermediate CA is to issue sector-specific CA certificates (banking, health, etc.). To date, only one general-purpose own-brand CA has been developed under this CA, called RACER.

1.1.- CA RACER (High Capillarity Network of Registration Authorities)
The main feature of RACER is that any agent can be used as a Registration Authority as long as it has received the required training and has been registered and audited to check it is able to properly fulfil the "obligations" stipulated in the Certification Policies.

Although **RACER** is a general-purpose multi-policy **CA** that issues final company certificates, most of the certificates issued by this CA are for specific projects and are business relationship certificates:

- Contractual relationship certificate
- Powers of representation certificate
- Powers of attorney certificate
- Electronic invoicing certificate
- Company certificate
- Electronic seal certificate

Because **RACER** is open, the above-listed certificates may have a slightly different structure to the certificate defined under JCC: Also under this **CA**, individual certificates can be requested that **do not determine** the individual's relationship or contract with a company and always guarantee the individual's identity as the Signatory/Subscriber, holder of the certificate.

RACER has no set regional scope, and so it can issue certificates anywhere there is a recognised RA that meets Camerfirma's requirements, always subject to current law and applicable to international trading relations.

1.2.2 Policy Authority

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

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

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

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

You can contact the Policy Authority (PA) at:

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

As regards the contents of this CPS, it is assumed the reader is familiar with the basic concepts of PKI, certification and digital signing. Should the reader not be familiar with these concepts, he/she is advised to gain some background knowledge on these concepts. The Camerfirma web site http://www.camerfirma.com provides general information about using digital signatures and digital certificates.

1.3. Identification

Name:	CPS Camerfirma SA
Description:	Document to fulfil requirements of Policies with ID numbers: 1.3.6.1.4.1.17326.10.8.* 1.3.6.1.4.1.17326.10.9.* 1.3.6.1.4.1.17326.10.10.* 1.3.6.1.4.1.17326.10.11.* 1.3.6.1.4.1.17326.10.12.* 1.3.6.1.4.1.17326.10.13.* 1.3.6.1.4.1.17326.10.14.* 1.3.6.1.4.1.14862.1.3 General policy for General State Administration certification.
Version:	3.2.5
Location:	https://policy.camerfirma.com/

1.4. Community and Scope of Application.

1.4.1 Certification Authority (CA).

This is the entity 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.

For the purpose of this CPS, every Certification Authority is managed by Camerfirma.

Information related to the CA is available on Camerfirma's web site http://www.camerfirma.com

1.4.2 Accreditation Authority

The accreditation authority will accept, authorise and supervise the certification authorities. This is the responsibility of the Spanish Ministry for Industry, Tourism and Trade.

1.4.3 Certification Service Provider (CSP).

This CPS defines a CSP as an entity that provides the specific services relating to the certificate life cycle and can manage one or more Certification Authorities and related services, such as issuing time stamps, providing signature devices or validation services.

For the purpose of this CPS, Camerfirma is the CSP.

1.4.4 Registration Authority (RA)

A Registration Authority (RA) is responsible for managing the requests, identification and registration of Certificate applicants, and any responsibilities established in the specific Certification Policies. RAs are authorities delegated by the CA, although the latter is ultimately responsible for the service. The CAs can carry out the RA's work at any time.

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

For the Chambers of Commerce Root Hierarchy (JCC):

- The Certification Authority.
- The Chambers of Commerce, Industry and Navigation, or the entities appointed by them. The delegated entities can carry out the registration process via:
    - **Physical verification points (PVP):** Entities that physically verify the certificate holder. Although they do not have registration powers, they are contractually bound to an RA so that the RA, based on the documentation collected by the PVP, registers and requests the certificate from the CA.
    - **Corporate RA:** An entity appointed by the RA to register Signatories/Subscribers belonging to the same organisation or entity within an RA's jurisdiction, for example: a corporation's employees, members of a corporate group, members of a professional body. The operators in these corporate RAs can only manage requests and certificates within that organisation's scope.
- The Public Administration, in the case of certificates issued under the **CA Camerfirma Public Administrations.**

For the Chambersign Hierarchy (JCS).

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

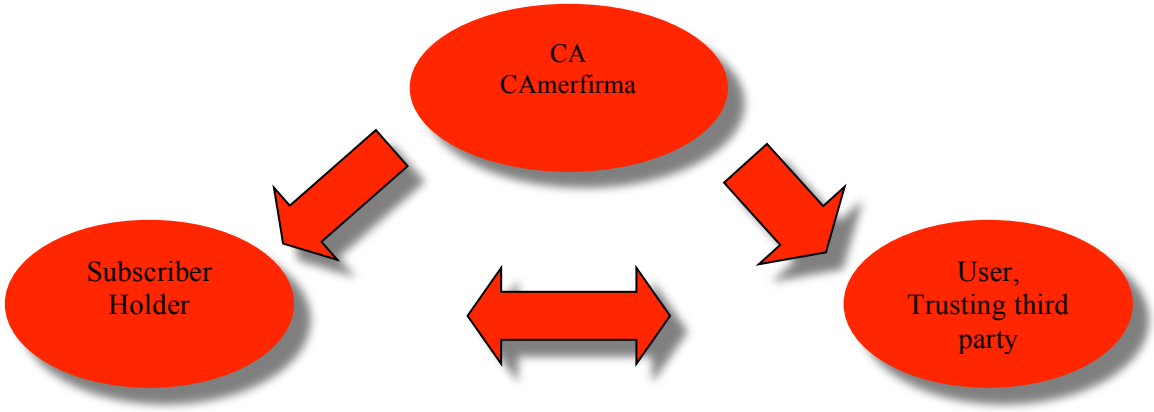
1.4.5 Signatory/Subscriber.

Signatory/Subscriber refers to the certificate holder, whether this is an individual or company. When it is issued in the name of a hardware device or software application, the individual/company requesting the issued certificate will be considered the Signatory/Subscriber.

Before the certificate is issued, the signatory/subscriber is considered the applicant.

1.4.6 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



1.4.7 Entity.

The Entity is the company or organisation with which the Signatory/Subscriber has a certain relationship, as defined in the ORGANISATION field in each certificate.

And so

- ✓ In **Individual relationship certificates**, the Entity is linked to the Signatory/Subscriber via a contractual relationship (labour, mercantile, as a member of professional body, 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 **Secure Server/Corporate Digital Seal 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.

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

1.4.8 Applicant.

Applicant refers to the individual requesting the Certificate from the Camerfirma CSP, either directly or via an authorised representative. Once the certificate has been issued, the applicant is considered the Signatory/Subscriber.

1.4.9 Person Responsible for Certificates

This CPS considers the certificate holder (the signatory/subscriber) to be the person responsible for certificates issued to individuals.

The CPS considers the individual making the request (the applicant) to be responsible for certificates issued to companies. This person must be identified in the certificate, even if the request is made via a third party. For certificates that contain powers of representation, this CPS considers both the Signatory/Subscriber and the represented person/Company to be the responsible party.

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

1.4.10 Scope of Application and Usage.

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

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

1.4.10.1 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 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 will be considered illegal, and the CA will be exempt from any liability due to the signatory or third party's misuse of the certificates in accordance with current law.

Camerfirma does not have access to the data for which a certificate is used. Therefore, due to lack of access to the message contents, Camerfirma cannot issue any appraisal regarding these contents and the signatory is consequently responsible for the data for which the certificate is used. The signatory will also be 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 in accordance with this paragraph or which could be interpreted as such by virtue of current law.

Camerfirma includes information in the certificate regarding usage restrictions, either in standard fields, under “key usage” and “basic constraints”, highlighted as critical in the certificate and therefore binding on any application using it, or via text included in the field such as "user notice”, which is “not critical” but binding on the certificate holder and user.

1.5. 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”

1.6. 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

In accordance with the stipulations of the Certification Policies and this CPS, and in accordance with current law regarding certification service provision, Camerfirma undertakes to:

- ✓ Adhere to the provisions of this CPS and the Certification Policies.
- ✓ Protect its private keys and keep them secure.
- ✓ Issue certificates in accordance with this CPS, the Certification Policies and the applicable technical standards.
- ✓ Issue certificates in accordance with the information in its possession and which do not contain errors.
- ✓ Issue certificates with the minimum content defined by current law for qualified or recognised certificates.
- ✓ Publish issued certificates in a directory, respecting 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, in accordance with current law.
- ✓ Publish this CPS and the Certification Policies on its web site.
- ✓ Report any amendments to this CPS and the Certification Policies to the Signatories/Subscribers and the RAs involved.
- ✓ 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 they are in its safekeeping, as necessary.
- ✓ Establish the data creation and custody systems in the aforementioned activities, protecting this data from being lost, destroyed or forged.
- ✓ Keep the data relating to the issued certificate for the minimum period required by current law.

2.1.1 RA

RAs are entities that Camerfirma appoints to carry out this task. The RAs also undertake the obligations 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.
- ✓ Check the identity of the Signatories/Subscribers and Applicants of the certificates.

- ✓ Check the accuracy and authenticity of the information provided by the Applicant.
- ✓ 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.
- ✓ Assume these obligations even when other entities are appointed (PVPs or Corporate RAs).

2.1.2 Certificate applicant.

An applicant requesting 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 proper identification.
- ✓ Ensure the accuracy and authenticity of the supplied information.
- ✓ Report any changes to the data provided to create the certificate during its validity period.
- ✓ Keep their private key secure.

2.1.3 The 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.
- ✓ Report any changes to the data provided to create the certificate during its validity period.
- ✓ Not to use the private key or certificate once Camerfirma requests or reports the suspension or revocation thereof, or once the certificate validity period has expired.

2.1.4 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 web site: http://www.camerfirma.com/camerfirmaPublic/index/Area-Usuario/Consulta-Validacion.html.

- Become familiar with and adhere to the guarantees, limitations and responsibilities regarding the acceptance and use of the trusted certificates, and agree to be subject to them.

2.1.5 Entity

In the case of certificates involving a business relationship, the Entity will undertake to request suspension/revocation of the certificate from the RA when the Signatory/Subscriber ends its business relationship with the organisation.

2.1.6 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/camerfirmaPublic/index/Area-Usuario/Consulta-Validacion.html.

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 shall be responsible for damages and losses caused to any person during their activities in the event they breach the obligations established in this Law.*
The certification service provider regulated herein shall be held liable in accordance with general regulations on contractual or non-contractual liability, as applicable, although the certification service provider must prove that it acted with due professional diligence."

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 in accordance with the terms and conditions established under current law and in the Certification Policies.

In this sense, Camerfirma is the only party responsible (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 request forms in PKCS#10 format.

Guaranteeing that the public and private keys work in conjunction with each other, using certified cryptographic devices and mechanisms.

That the certificate requested and the certificate delivered match.

Any liability established under current law.

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

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.
- Properly identifying applicants, who must be trained or authorised to request a digital certificate.
- Checking the validity of the applicant's details and the Entity's details, if there is a contractual relationship or powers of representation.
- Accessing the Registration Authority application to process requests and issued certificates.

2.- Obligations once the certificate has been issued.

- Signing Digital Certification Service Provision agreements with applicants.
- Maintaining the certificates while they are still in force (expiry, suspension, revocation).
- Filing copies of submitted documentation and the agreements signed by the applicants in accordance with the Certification Policies published by Camerfirma and current law.

The RAs are responsible for any consequences due to breach of or failure to properly fulfil their registration duties, and undertake to adhere to Camerfirma's internal regulations (Policies and CPS), which the RAs must keep in mind and which they must use as guidelines.

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, in accordance with the agreement signed with the RAs. Although in legal terms the CA is the legal entity responsible in relation to the Signatory, an Entity or Trusting Third Party, and holds a public liability policy for this purpose, in accordance with the agreement in force and the Policies the RA assumes the contractual obligation of "identifying and authenticating the Applicant and, if necessary, the Entity" and must therefore accept responsibility for any breach on their part in relation to Camerfirma.

Of course, it is not Camerfirma intention to burden the RAs with the entire weight of responsibility for any damages due to a breach of the duties delegated to the RAs. For this reason, in the same way as for the CAs, the RA is subject to a control system imposed by Camerfirma, not only based on checking the files and filing systems the RA receives, but also audits to evaluate the resources used and its knowledge and control over the operational procedures used to provide the RA services.

2.2.1 Exemption from liability

In accordance with current law, the responsibility assumed by Camerfirma and the RA does not apply in cases in which certificate misuse is caused by actions attributable to the Signatory and the Trusting Third Party due to:

- Not having provided the right 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 their 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 Trusting 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 allowed use and limited amount of transactions, or when it does not consider the certificate's validity situation.
- 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 shall neither be held responsible, under any circumstances, in the following situations:

- Warfare, natural disasters or any other case of Force Majeure.
- The use of certificates in breach of current law and the Certification Policies.

- The misuse or fraudulent use of the certificates or CRLs issued by the CA.
- Use of the information contained in the Certificate or CRL.
- Damages caused during verification of the causes for revocation/suspension.
- Due to the contents of messages or documents signed or encrypted digitally.
- 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 by including the extension **"qcStatements"**, (OID 1.3.6.1.5.5.7.1.3), as defined in **RFC 3039**. The monetary value expression shall be in keeping with section 5.2.2 of standard **TS 101 862** of the ETSI (European Telecommunications Standards Institute, *www.etsi.org*).

Unless the aforementioned certificate extension states otherwise, the maximum limit Camerfirma allows in financial transactions is 0 (zero) euros.

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 Trusting Third Party, and to third parties, amounting to a total of **€3,700,000.**

2.4. Interpretation and enforcement

2.4.1 Law

The enforcement, interpretation, amendment or validity of this CPS shall be 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 this case, the aforementioned clause shall be considered not included.

2.4.3 Notification

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

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 Court Arbitration in accordance with its Regulations and Statutes, entrusted with the administration of the arbitration and the nomination of the arbitrator or arbitrators. The parties undertake to comply with the decision reached.

2.5. Prices

2.5.1 Price for certificate issuing and renewal.

The prices for certification services or any other related services are available and updated on the Camerfirma web site
http://www.camerfirma.com/camerfirmaPublic/index/certificados.html.

The specific price is published for each type of certificate.

2.5.2 Prices for access to certificates.

Access to certificates is free-of-charge; although CA Camerfirma applies controls to avoid mass certificate downloads. Any other situation that Camerfirma deems must be considered in this respect will be published on the Camerfirma web site http://www.camerfirma.com.

2.5.3 Prices for access to information relating to the status of certificates or renewed certificates.

Camerfirma provides free access to information relating to the status of certificates or revoked certificates via certificate revocation lists or via its web site http://www.camerfirma.com/camerfirmaPublic/index/Area-Usuario/Consulta-Validacion.html

Camerfirma currently offers the OCSP service free-of-charge but reserves the right to invoice these services. If invoiced, the prices of these services will be published at http://www.camerfirma.com/camerfirmaPublic/index/Servicios/OCSP.html.

2.5.4 Prices for access to the contents of these Certification Policies.

Access to the content of this CPS is free-of-charge, on the Camerfirma web site https://policy.camerfirma.com.

2.5.5 Refund policy.

CA 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.

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.

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 issuing process, either via the physical contract or the condition acceptance process prior to making the request.

2.6.1.3 Distribution of the certificates.

The issued certificates can be accessed as long as the **Signatories/Subscribers provide their consent** on the web site:

http://www.camerfirma.com/camerfirmaPublic/index/Area-Usuario/Consulta-Validacion.html

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.

CA Camerfirma **publishes the certificates** immediately after they have been issued, provided the Signatories/Subscribers have given their approval.

CA Camerfirma issues and publishes **revocation lists** regularly in accordance with the following table, and immediately after a revocation has taken place.

AC	Issued every...	Duration
CHAMBERS OF COMMERCE ROOT	180 days	180 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	30 days	30 days

CHAMBERSIGN ROOT	**180 days**	**180 days**
CA CAMERFIRMA	180 days	180 days
RACER	24 hours	48 hours

CHAMBERS OF COMMERCE ROOT -2008	**365 days**	**365 days**
CAMERFIRMA CHAMBER OF COMMERCE CERTIFICATES - 2009	24 hours	48 hours
CAMERFIRMA PUBLIC ADMINISTRATIONS- 2010	24 hours	48 hours
CAMERFIRMA CORPORATE SERVER - 2009	24 hours	48 hours
CAMERFIRMA CODESIGN - 2009	24 hours	48 hours
CAMERFIRMA TSA - 2009	30 days	30 days

CHAMBERSIGN ROOT - 2008	**365 days**	**365 days**
CAMERFIRMA	365 days	365 days
RACER	24 hours	48 hours

Camerfirma immediately publishes any changes to the **Policies and CPS** on its web site https://policy.camerfirma.com, where it maintains a version log.

2.6.3 Access control

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

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

2.7. Audits

Camerfirma is committed to the security and quality of its services.

Camerfirma objectives in relation to security and quality have essentially involved receiving the **ISO/IEC 27001:2005, ISO/IEC 2000-1:2007** certificates and subjecting its certification system, and fundamentally the RAs, to internal audits every two years, to ensure compliance with internal procedures.

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

Camerfirma successfully passed a standard inspection procedure by the Ministry for Industry in **2007**. The Ministry for Industry is the regulatory body responsible for supervising the activities undertaken by Spanish certification service providers.

The Registration Authorities belonging to both hierarchies are subject to an internal audit process. These audits are conducted regularly, at least every two years. The frequency of audits (one or two years) on the registration authorities is calculated in accordance with the number of issued certificates and number of registration authorities.

2.7.1 Audit frequencies

See 2.7

2.7.2 Auditor identification and rating

The audits are conducted by the external reputed company.

- For the WEBTRUST Ernst & Young audit.
  http://www.ey.com/ES/es/home.
- For ISO27001 AENOR audits.
  http://www.aenor.es/aenor/inicio/home/home.asp
- For internal Start-Up audits.
  http://www.seguridadinformacion.com/

2.7.3 Relationship between the auditor and the CA

The audit companies used are reputed companies with specialist IT audit departments, which rules out any conflict of interest that could affect their work with the CA.

2.7.4 Topics covered in the audit

The audit checks:

a) That Camerfirma has a system that guarantees service quality.
b) That Camerfirma complies with the requirements of the Certification Policies that regulate the issuing of the different digital certificates.
c) That the CPS is in keeping with the provisions of the Policies, with that agreed by the Authority that approves the Policy and as established under current law.
d) That Camerfirma properly manages its information systems.
e) In the EV certificates, the internal audit will take a sample of 3% of the issued certificates to analyse them thoroughly.

2.7.5 Auditing the Registration Authorities

Every RA is audited. These audits are conducted at least every two years and check compliance with the Certification Policy requirements in relation to undertaking the registration duties established in the signed service agreement.

As part of the internal audit, samples will be taken of the issued certificates to check they have been processed properly.

Reference documentation:

IN-2010-04-12-RA Security Evaluation Procedure
IN-2010-04-15-Ficha de la visita de evaluación.doc
IN-2010-04-16-Lista de Chequeo
IN-2006-03-08-Procedimiento Labores de AR.
IN-2010-04-17-Informe de evaluación

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 confidential, unless established by law.

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

Reference documentation:

IN-2005-02-04-Política de Seguridad.

IN-2006-02-03-Normativa Seguridad.

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

Reference documentation:

IN-2006-05-11-Conformidad de Requerimientos legales

2.8.2 Type of information considered not confidential

Camerfirma considers the following information not confidential:

a) The contents of this CPS and the Certification Policies
b) The information contained in the certificates provided the Signatory/Subscriber has given consent.
c) Any information that must be published by law.

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 web site:
http://www.camerfirma.com/camerfirmaPublic/index/Area-Usuario/Consulta-Validacion.html

2.8.4 Sending information to the Competent Authority

Camerfirma will provide the information that the competent authority requests in compliance with current law.

2.9. Intellectual property rights

Camerfirma owns the intellectual property rights for this CPS.

3. Identification and Authentication

3.1. Initial registration

3.1.1 Types of names

The Signatory/Subscriber is described in the certificates by a DN (distinguished name) in accordance with the X.500 standard. The DN field descriptions are shown in each of the certificate profile sheets.

3.1.2 Pseudonyms

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

The calculation of the pseudonym in certificates in which it is allowed is done so that it unmistakeably identifies the real **certificate holder, attaching an organisation 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

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 certificates for the same subject.

A subscriber could have more than one certificate, provided that; one of the request existent values would be different from an issued certificate:

CIF. Organisation VAT Number
NIF. Subject ID number
Certificate Type. X509 Description field.

As exception this CPS allows a RA operator validate a certificate request when already there was a valid certificate with the same three values, when a different value are found in the field TITLE and/or ORGANITATIONAL UNIT.

3.1.5 Name dispute settlement procedure

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

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

Camerfirma complies with section 2.4.4 of this CPS.

3.1.6 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 the issuing of certificates.

3.1.7 Methods of proving ownership of private key.

Camerfirma uses various circuits for the issue of 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

   They are given to the subscriber in person or by mail via protected files, using Standard **PKCS#12**. Security is guaranteed because the file access key that allows it to be installed in applications is delivered via different means to the one used to receive the PKCS#12 file (mail, telephone, delivery in person, SMS, etc.)

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

b) Keys created by subscriber.

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

   When the subscriber creates its own keys in a cryptographic device and asks Camerfirma to issue a digital certificate with a key creation policy on a hardware device, the subscriber must include a declaration with the request which specifies:

   - The process followed to create the keys

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

This report can be written and signed by a third party (company performing the installation for the customer) or by the customer in an affidavit.

The report must be approved before the certificate is issued by the Camerfirma technical department supervisor.

CA Camerfirma reserves the right to consider the external auditor's guarantee as valid, or to reject it.

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

In recognised certificates:

- Applicant's ID:
  The Signatories/Subscribers are required to introduce themselves in person when they are also the Applicant, or the Applicant's representative when this is a company, and they must also show their National Identity Document, residency card or passport. Physical introduction is not required for these certificates in the cases established in Law 59/2003.

- Entity's ID:
  The RA will request 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. No documentary proof of the entity's existence will be required when this is regulated by law.

- Proof of 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 will be submitted. The RA can also check the status and level of the applicant's powers of representation online.

For Special Power of Attorney Certificates, the powers are described in a table with different headings, which are included in the certificate in two ways: One, by including the powers of representation headings in the TITLE field, and two, via a link in the USER NOTICE field to the scanned deeds 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 **Company certificates**, where the Signatory/Subscriber and the Applicant are different, documentary proof of the Applicant's sufficient powers to request the certificate on the Signatory/Subscriber's behalf is required, in the form of a certificate from the public register issued in the last **10 days** or via online consultation of the public register information made by the RA.

For **Public Employee/Electronic Office and Seal Certificates**, documentation proving that the public administration, public body or public entity exists is not required because this identity is part the General State Administration or other State Public Administrations corporate scope. The identity documents of the person who is acting on behalf of the Public Administration, body or entity is required. The RA will identify the Applicants from their national identity document and proof that they are an employee of the Public Administration, body or entity, which must also specify their tax identification number.

For technical or component certificates:

For **OV (Organisation Validation) Secure Server Certificates** the following is checked:

1. **The entity's existence** by accessing public registers (www.registradores.org; www.rmc.es), Camerdata (www.camerdata.es) or the Spanish Tax Office databases (www.aeat.es).

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, so Camerfirma will stop issuing certificates of this kind from **1 November 2015**. In any case, issued certificates of this type will be revoked if their expiry date is later than October 2015). The customer will be notified of this before the certificate is issued.

Domain information will be taken from the WHOIS service of the registrar of the domain for which the rules established in the ccTLD are applied.

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

The certificate is delivered via email to at least the administrative and technical supervisors that appear in the domain databases.

Proof of the issuing of **Corporate digital seal certificates** is provided as follows: The existence of the company/entity is checked in the AEAT, Camerdata or public register databases, in the same way as for the OV Secure Server Certificates mentioned above. The applicant's email address must come from an account with a domain related to the company or body that made the request.

The certificate will be delivered to that email address. If a file is delivered in PKCS12 format, the activation code will be provided by telephone. The telephone number will be found by accessing https://www.paginasamarillas.es or calling the telephone number information service. This information will be included in the certificate issuing report.

The holder field (CN) in corporate seal certificates can include: the company's name, the name of the application for which the certificate has been created or an internal reference. Camerfirma will not check this information.

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

For **CodeSign certificates**, the same checking system is used as for Digital seal certificates.

Encryption certificates will be issued online, using a valid recognised certificate for this purpose.

In accordance with 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 will only be carried out when the certificate is for exclusive encryption use.

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

1. The Signatories/Subscribers, or an Applicant's representative if this is an entity, must introduce themselves in person and present an identity document or passport.
2. The RA will request the required documentation depending on the type of entity in order to identify it. The entity's business activity must be proven. This will be checked by accessing the commercial registry or other business activity registers.
3. Submission of authorisation signed by an entity's representative, who will act as the Applicant.
4. Documentation proving the Applicant's capacity.

For these certificates, the RA must also check:

1. The entity's existence:
    - By accessing public registers (www.registradores.org; www.rmc.es), Camerdata (www.camerdata.es) or the Spanish Tax Office databases (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.
    - 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 issuance 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 will check the information is accurate. The certificate will include this information as defined in the reference certification policies.

Each entity type must submit the appropriate documentation in keeping with its legal status to prove its existence, as described on the Camerfirma web site.

http://www.camerfirma.com/camerfirmaPublic/index/buscadores/buscador_documentos.html

Certificates specified as EV are checked each month by an internal auditor who will ensure they have been issued properly.

3.2. Key renewal

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

When qualified or recognised certificates for electronic signatures are renewed, no physical presence is required because Law 59/2003 on Electronic Signatures allows up to a period of **five years** since the last registration in person. Once the period established by the subscriber has lapsed, the same physical issuance process as the first time must be applied. If less than five years have passed since the certificate was issued, Camerfirma does not consider the holder's physical presence necessary, regardless of the issued certificate's expiry date.

Technical certificates (secure server, corporate seal and code sign) cannot be renewed, a new certificate must always be issued.

Camerfirma gives four warnings (30 days, 15 days, seven days, one day) via email to the subscriber that the certificate is about the expire, suggesting renewal thereof. If the active certificate to be renewed expires before the renewal takes place, a new certificate must be issued.

The renewal process can be initiated from the Camerfirma web site http://www.camerfirma.com/camerfirmaPublic/index/Area-Usuario/Renovar-Certificado.html. The active certificate to be renewed is required to carry out this process.

- Once the certificate being renewed has been identified, the application gives 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 request is included in the RA application. Once the operator has checked the information and payment, he/she requests the CA to issue the certificate.

- **The CA issues a new certificate, taking the expiry date of the certificate being renewed as the start date of this new certificate.**

3.3. Re-issuance following a revocation

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

When the renewal takes place due to certificate replacement or an issuing error, renewal is possible following a revocation. As long as the current situation is shown, the supporting documentation submitted to issue the replaced certificate will be reused and the physical presence will no longer be required, if this were necessary due to the type of certificate. Camerfirma will update the number of years since the last physical presence to the status of the certificate being replaced, just as if this process had been the result of an ordinary renewal.

3.4. Request for revocation

The method of making revocation requests is established below.

4. Operational Requests

4.1. Certificate request

Certificate requests are submitted via the application forms at

http://www.camerfirma.com/camerfirmaPublic/index/certificados.html.

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

Batch requests are also allowed. In this case, the applicant will send the RA a file with a structure designed by Camerfirma containing the applicants' details. The RA will upload these requests in the management application.

When the applicant creates the keys, the certificates are requested by submitting a standard PKCS#11 or CSR certificate issuance request together with the additional request information.

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.

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 issuance, renewal and revocation services. Calls to these WS are signed by an authorised registration operator, and so the transactions are carried out directly on the platform.

4.2. Cross certification request.

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

4.3. Certificate issuance

Qualified or Recognised certificates: The standard procedure is started by filling in a form online and confirming the information. The application will respond by sending an email to the subscriber requesting their physical presence at the RA's facilities, or at an agreed place, with the required documentation. If the request is made via an electronic identity card or a recognised certificate that Camerfirma accepts, physical presence will not be required.

The RA operator will check the applicant's documentation and check that the services have been paid for, if necessary. Once this is complete, the RA operator will use the electronic signature to check that the certificate has been issued.

The following cases are possible:

Certificates via Software: The user receives a link via the email account related to the certificate in order to create and download the certificate. The product code provided with the contract and an installation code sent in a separate email or via SMS together with a revocation code will be required to install it.

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

Certificates via HW (Secure Signature Creation Device):

- **Cryptographic Card or Token:** The user receives the signature device with the certificates and keys at the RA's offices.

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

  The subscriber will receive the cryptographic device access code and unlocking code, as well as a revocation code, via the linked email account.

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

- **Certificates via centralised key management platform.** CA Camerfirma provides a centralised key management system. The keys are created in an **HSM FIPS 140 2 level three** where they are stored for use by the public key certificate holders.

  In this case the request is made in accordance with the standard procedure, i.e. via an online form. On the platform, the Registration Authority operator will choose to create the keys in a centralised cryptographic device. For this purpose, the operator's work station must be configured with the CSP

(Cryptographic Service Provider) for the centralised key creation device.

The subscriber will have client software installed on their PC to allow their local keystore to be linked securely to the keys stored on the centralised PC.

The subscriber will receive the private key activation codes by email. This means the subscriber has 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.

- **Certificates via mobile phone:** Another certificate issuance option is delivery via a mobile phone. This is currently only available on phones on the Vodafone network. The system is not operational at this time. In this case, the subscriber must have an authorised mobile device. CA Camerfirma sends an order to the telephone operator management system so that the keys are created on the device's SIM card. The telephone operator management system then sends a PKCS10 request to Camerfirma, who issues the corresponding certificate.

Requests via WS: Requests can be received via duly signed calls to the STATUS application WS services layer.

Batch requests: Certificates can also be requested in batch processes. These batches are delivered to the RA in a structured file, and are then entered into the management platform. Once the RA operator has compiled the documentation and checked the identity, he/she validates the certificates one-by-one or in batches.

For technical certificates (Corporate Seal, Secure Server and Code Sign) no physical presence is required for issuance. The documentation just needs to be sent to the RA office. Once the documentation has been checked and payment made, if applicable, CA Camerfirma issues a certificate, either by issuing a PKCS12 file or a PKCS7 file if the customer has delivered a PKCS10.

Further information is available on the Camerfirma web site:
http://www.camerfirma.com/camerfirmaPublic/index/certificados/COMPONENTES.html

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

Certification policies for issuing SSL EV certificates to which this CPS is subject ("CA/Browser Forum Guidelines for Issuance and Management of extended validation certificates") require that each EV certificate issue request be 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 CA Camerfirma internal audit department will check the documentation and proceed with the final certificate validation and issuance.

The subscriber can use their own resources to create the keys in cryptographic device and deliver the request to Camerfirma in PKCS10 format to issue the certificate. This process can be used for any type of certificate, although it is common in secure server certificate requests where a file is usually submitted in PKCS#10 or CSR format.

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

- ✓ A link to the web page where the certificate will be created in PKCS#12 format.
- ✓ A PIN required to install the keys and certificate. The Signatory/Subscriber can choose the option to send by SMS on the application form.
- ✓ The Signatory/Subscriber will also require a code for the key and certificate creation process, which will be printed in the contract signed with the RA and the CA.

If the subscriber creates the key, he/she will give Camerfirma a standard PKCS#10 request and Camerfirma will send the user a certificate in PKCS#7 format. In this case, the subscriber must provide Camerfirma with an audit report confirming that the keys have been created in a hardware environment, before Camerfirma issues the certificate, otherwise Camerfirma will consider the certificate issued via software.

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

http://www.camerfirma.com/camerfirmaPublic/index/certificados/COMPONENTES/CX-Info.html

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

4.4. Certificate acceptance.

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

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

4.5. Certificate suspension and revocation.

4.5.1 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 a cause for revocation or suspension will become 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.

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

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

4.5.2 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 will be revoked where:

There are circumstances affecting the information contained in the certificate

- Any of the details contained in the certificate are amended.

- Errors are detected in the data submitted in the certificate request or there are changes to the verified circumstances for the issue of the certificate.
- An error is detected in any of the details contained in the certificate.

There are 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.

There are 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.

There are 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 issuance of the certificate to the subscriber or certificate manager.
- The applicant breaches part of the requirements established for requesting 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 incapacity or death of the subscriber or certificate manager.
- There is a termination of the certificate subscribing company and expiry of the authorisation provided by the subscriber to certificate manager, or termination of relationship between the subscriber and certificate manager.
- The subscriber requests to revoke the certificate, in accordance with the provisions of this CPS.

Other circumstances

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

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

4.5.3 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.

Anyone established in the specific certification policies.

4.5.4 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/camerfirmaPublic/index/Area-Usuario/Revocar-Certificado.html

- ✓ By physically going to the RA's offices during opening hours, showing the Signatory/Subscriber or Applicant's **National Identity Card**.
- ✓ By sending Camerfirma a document signed by one of the Entity's representatives requesting certificate revocation.
- ✓ For **secure server, corporate seal or code sign certificates**, this revocation can be requested by email, using the address used to request issuance of the certificate, sending the revocation request to gestión_soporte@camerfirma.com. The Camerfirma operator 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/camerfirmaPublic/index/Area-Usuario/Revocar-Certificado.html

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 will be available 24 hours a day, seven days a week. In the event of a system failure, or any other circumstance out of Camerfirma's control, Camerfirma will make every effort to ensure the services are not down for more than **24 hours**.

4.5.5 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.

4.5.6 Suspension

When a certificate suspension takes place, Camerfirma will have **one week** to decide on the certificate's final status: 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, a notice will be sent to the Signatory/Subscriber by email specifying the time of suspension and the reason.

The RA will receive an email from the system notifying that the certificate has been suspended.

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

4.5.7 Procedure to request suspension

The suspension request must be made in accordance with the procedure described in section 4.5.6 of this CPS.

4.5.8 Suspension period limits

A certificate shall 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.

4.5.9 CRL issuance frequency

See 2.6.2.

4.5.10 CRL checking requirements

Trusting third parties must check the status of certificates they are going to trust, and in any case must consult the latest CRL which can be downloaded from the following web site:

http://www.camerfirma.com/camerfirmaPublic/index/Area-Usuario/Consulta-Validacion.html.

Camerfirma always issues CRLs signed by the CA that issued the certificate. There are also links to the CRL in the certificate extension "CRL distribution points".

4.5.11 Availability of online service to check revocation

CA provides an online service to check revocations at:

http://www.camerfirma.com/camerfirmaPublic/index/Area-Usuario/Consulta-Validacion.html

also via OCSP consultations at:

http://www.camerfirma.com/camerfirmaPublic/index/Servicios/OCSP.html

The addresses to access 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 to which the service is provided. The technical access data and the OCSP response validation certificates are published on the Camerfirma web site
http://www.camerfirma.com/camerfirmaPublic/index/Servicios/OCSP.html

These services will be available **24 hours a day seven days a week**.

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

4.5.12 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 that they want to consult if this is accessed online.

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

http://www.camerfirma.com/camerfirmaPublic/index/Servicios/OCSP.html

4.5.13 Other methods of distributing revocation information

The means that Camerfirma makes available to system users will be published on its web site: http://www.camerfirma.com/camerfirmaPublic/index/Area-Usuario/Consulta-Validacion.html.

As an example, an extra online certificate checking service is provided:

> Consultation of certificate status via "Web Service" in accordance with AEAT requirements.

4.5.14 Checking requirements for other methods of distributing revocation information

Not stipulated

4.5.15 Special revocation requirements due to compromised key security

Not stipulated

4.6. Security Control Procedures

Camerfirma is subject to the annual validations established by the ISO27001 standard, which regulates the establishment of suitable processes to ensure proper security management in information systems.

4.6.1 Types of recorded events

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

The following events will be recorded:

- ✓ System switching on and off.
- ✓ Creation, deletion and setting up of passwords or changed privileges.
- ✓ Attempts to log in and out.
- ✓ Attempts at unauthorised access to CA's system online.
- ✓ Attempts at unauthorised access 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.

4.6.2 Log processing frequency

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

Camerfirma maintains a system that guarantees:

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

4.6.3 Storage periods for audit logs

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

4.6.4 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 ensure 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.

4.6.5 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

4.6.6 Audit data collection system

Event audit information is collected internally and automatically by the operating system and certificate management software.

4.6.7 Notifying the party that caused the event

Not stipulated.

4.6.8 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 ISO27001 certificate and are included in the Risk analysis document, 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.

4.7. Log files

4.7.1 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.

- ✓ Any data related to certificates, including contracts with signatories and their identification details.
- ✓ Requests to issue and revoke certificates.
- ✓ 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 properly filing all this material.

4.7.2 File storage period

Certificates, contracts with Signatories/Subscribers and any information relating to the Signatory/Subscriber's identification and authentication will be kept for at least **15 years**.

4.7.3 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**

4.7.4 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 restricted to authorised personnel.

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

4.7.5 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 which describes the time settings for the devices used for the issue of certificates.

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

4.7.6 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

4.7.7 Procedures to retrieve and verify filed information

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

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

4.8. Changing the key

The CA private key will be changed before it expires. The old CA and private key will only be used to sign CRLs while there are active certificates issued by the old CA. A new CA will be created with a new private key and a new DN.

The subscriber's keys are changed by starting a new issuance procedure (see section 3.2 of this CPS).

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

4.9. 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.

If the root key security is compromised, this must be considered a separate case in the contingency and business continuity plans. If the keys are replaced, this incident affects recognition by the different applications and private and public services. Recovering the validity of keys in business terms will mainly depend on the duration of these processes. The contingency and business continuity plans will only deal with operational aspects to ensure 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 will be considered unavoidable unless there is a breach of obligations on Camerfirma's part in implementing these processes.

4.9.1 An entity's key is compromised

The Camerfirma contingency plan considers any situation where the compromised security of the CA's private key is a disaster.

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 will be informed.
- They will be informed that the certificates and information relating to the revocation status that are signed using this key are not valid.

4.9.2 Security installation following a natural or other type of disaster

Camerfirma will reinstate the critical services (revocation and publication of revocations) in accordance with the contingency and business continuity plans.

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

4.10. Termination of CA activity

Before the Camerfirma ceases its activity, it 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 issuance 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 will be 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 ISO27001 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 transactions are stored.

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

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

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

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

5.1.1 Location and building

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

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

5.1.2 Physical access

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

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

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 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 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.

5.1.6 Storage systems.

Each dismountable storage device (tapes, cartridges, 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.

Printed matter and paper: Shredders or waste bins provided for this purposes, later destroyed via controlled means.

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

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

5.1.8 External backup

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

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

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

5.2. Procedural controls

5.2.1 Roles of trust

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

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 requests from the subscriber.

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 formed by the following modules:

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

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

Request Management Module, for which the specific page manager services will be 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:

- Request module
- RA module
- OCSP module
- TSA module
- Database module
- Key management module.

The switching on process will be carried out in reverse.

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

5.3. Personnel security controls

5.3.1 Background, qualifications, experience and accreditation requirements

All personnel undertaking tasks classified, as duties of trust must have worked at the workplace for at least **one year** and have an open-ended employment contract.

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

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

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

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

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**.

5.3.3 Training requirements

Personnel undertaking duties of trust must have been trained in accordance with the Certification Policies. There is a training plan that is part of the ISO27001 controls.

Registration operators who validate EV secure server certificates will receive specific training in accordance with the special regulations on the issuance of these certificates.

5.3.4 Information updating requirements and frequency

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

5.3.5 Task rotation frequency and sequence

Not stipulated

5.3.6 Penalties for unauthorised actions

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

5.3.7 Personnel hiring requirements

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

5.3.8 Documentation given to personnel

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

Any documentation that employees require will also be supplied at any given time 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

A device is used to create the CA's keys, which complies with the requirements established in **FIPS 140-1, level 3.** The device details are: Advanced Crypto Module **(ACM)2** by **RETEMSA.** They include HSM Eracom with the same certification for issuing OCSP responses and time stamps.

Camerfirma has purchased new cryptographic modules supplied by nCipher to replace the current RETEMSA modules. These new modules will store new root keys which will replace the current ones and are certified in accordance with **FIPS 140-2, level three.**

The keys for the CA that issues secure server and timestamp certificates were created in a secure environment via software mechanisms and under dual control.

The keys for the CA that issues EV server certificates were created in a cryptographic device certified in accordance with **FIPS 140-1, level three.** The device details are: Advanced Crypto Module **(ACM)2** by **RETEMSA.**

The keys for the CA that issues CodeSign certificates were created in a device that complies with the requirements described in **FIPS 140-1, level three.** The device details are: Advanced Crypto Module **(ACM)2** by **RETEMSA.**

ROOT **Chambers of Commerce Root**	**2048**	**34 years**
CAMERFIRMA	2048	30 years
Relationship,	1024	Two years.
Representative	1024	Two years
Company	1024	Two years
Power of Attorney	1024	Two years
Invoice	1024	Two years
Encryption	1024	Depends on the signature certificate
CAMERFIRMA PUBLIC ADMINISTRATIONS	2048	12 years
Public employee, mid-level	1024	Three years
Public employee, high-level	2048	Three years

Administration Electronic Seal, mid-level	1024	Three years
Administration Electronic Seal, high-level	2048	Three years
Electronic office, mid-level	1024	Three years
Electronic office, high-level	2048	Three years
CA Corporate Server EV	2048	25 years
Server Certificate	1024	1,2 years
CA Express Corporate Server	2048	30 years
Server Certificate	1024	1,2,3 years
CA Electronic Seal	1024	1,2,3,4 years
CA CodeSign	2048	30 years
Codesign certificate	1024	1,2,3,4 years
CA Timestamp	2048	30 years
CA TSU	1024	Five years
Token		
CA ROOT-Chambersign Global Root	**2048**	**34 years**
CAMERFIRMA	2048	30 years
RACER	2048	20 years
Domain server	1024	1,2,3,4 years
Electronic invoicing	1024	1,2,3,4 years
Individual	1024	1,2,3,4 years
Individual, contractual relationship	1024	1,2,3,4 years
Corporate seal	1024	1,2,3,4 years
Individual, contractual relationship, Representative	1024	1,2,3,4 years
Encryption	1024	1,2,3,4 years
Company	1024	1,2,3,4 years
Individual, contractual relationship, power of attorney	1024	1,2,3,4 years

New ROOT 2008 keys to replace old ones stored in RETREMSA HSM. They were created in an event in on which there is detailed documentation. The keys were generated in the new nCipher cryptographic modules.

ROOT Chambers of Commerce Root 2008	**4096**	**30 years**
CA ROOT-Chambersign Global Root 2008	**4096**	**30 years**

Reference documentation:

CONF-00-2012-01/06/07/08 **MINUTES from key creation events**.
CONF-00-2012-02/04 **Key generation SCRIPTS**.
CONF-00-2012-05 **E&Y 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 **PKCS#12** software format.

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

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

If subscribers creates the keys on their own cryptographic device, Camerfirma will request a technical audit report that will be appraised before a certificate with keys created on a hardware device is issued. If the subscriber does not provide the document or if it is not satisfactory, Camerfirma will only be able to issue a certificate classified as keys created on a software device.

Notes on the centralised key management system:

If a centralised signing system is implemented, a storage device will be used for the user keys, which must comply with at least FIPS-140-2 level three.

6.1.2 Delivering the public key to the certificate issuer

The public key will be 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 will be available to users on Camerfirma's web site.

http://www.camerfirma.com/camerfirmaPublic/index/Area-Usuario/Claves-Publicas.html

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 in accordance with RFC 3280 y PKCS#1. The algorithm for creating keys is the RSA.

6.1.7 Checking parameter quality

Module Length = 2048
Key creation algorithm: rsagen1
Padding scheme: emsa-pkcs1-v1_5
Hash functions: SHA-1.

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 CA keys have been created in an Advanced Crypto Module (ACM)2 by RETEMSA, certified in accordance with **FIPS-140-1 level three**.

For the new ROOT 2008 keys, a new nShield PCI 500 F3 by nCipher device has been used. This device complies with **FIPS 140-2 level two and level three**.

6.1.9 Purpose of key use

The chart below describes the key uses for different issued certificates. The solution adopted to differentiate between uses is:

Certificates for DS bit authentication (can be combined with other uses).

Certificates for DS + NR bit electronic signature (can be combined with other uses).

Exclusive NR bit recognised signature certificates (CANNOT be combined with other uses). Camerfirma does not currently issue exclusive recognised electronic signature certificates but this model sets out the guidelines for when it is included.

CA	DS	NR	KE	DE	KA	KCS	CRLS	EO	DO
ROOT Chambers of Commerce Root						x	x		
CAMERFIRMA	x					x	x		
Relationship,	x	x	x*	x*	x				
Representative	x	x	x*	x*	x				
Company	x	x	x*	x*	x				
Power of Attorney	x	x	x*	x*	x				
Invoice	x	x							
Encryption				x					
CAMERFIRMA PUBLIC ADMINISTRATIONS	x					x	x		
Officer F		x							
Officer A	x								
Officer X			x	x					
Officer M	x	x	x*	x*					
Admin Seal A	x	x	x	x					
Admin Seal M	x	x	x	x					
Electr. Office M	x		x						
Electr. Office A	x		x						
CA Corporate Server EV						x	x		
Server Certificate	x	x	x	x					
CA Express Corporate Server	x					x	x		
Server Certificate	x	x	x	x					
CA Electronic Seal	x	x	x	x					
CA Code-Sign	x	x							
CA Timestamp	x					x	x		
TSU	x	x							
CA ROOT-Chambersign Global Root						x	x		
CA CAMERFIRMA	x					x	x		
RACER	x		x*	x*	X*				

DS Digital Signature
Non Repudiation, “ContentCommitment”
KE Encryption de Clave
DE Data Encryption
KA Key Agreement

KCS Certificate Signing
CRLS CRL Signing
EO Encryption Only
DO Deciphering Only

(*) Although technically possible, Camerfirma does not accept responsibility for its use for these purposes.

6.2. Protecting the private key

The CA's private key

The CA's private key is kept and used in a secure cryptographic device that complies with **FIPS 140-1 level three** requirements for the **JCC and JCS** hierarchies.

A RETEMSA ACM2 device, **approved in accordance with FIPS 140-1 level three**, is used to manage CA keys.

An **Eracom** device in accordance with **certificate FIPS 140-1 level three** is used for OCSP and TSA authorities.

When the CA key is outside the device it is kept encrypted and shared between various devices.

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.

For the new ROOT 2008 keys, a new nShield PCI 500 F3 by nCipher device has been used. This device complies with **FIPS 140-2 level two and level three** specifications.

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 will provide 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 signature.

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

Notes on the centralised key management system:

If a centralised signing system is implemented, a storage device will be used for the user keys, which must comply with at least FIPS-140-2 level three. The key is activated remotely using a secret password that the management platform sends to the certificate holder or the person responsible for the keys, and ensuring only this person has control of the private key.

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. In accordance with 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 subscribers' private keys when they are created by the PSC and are subject to Law 59/2003 on Electronic Signatures. For certificates created on hardware, the user creates and stores the private key on the cryptographic card delivered by the PSC.

Camerfirma will only store a copy of the subscriber's private key when it is used “exclusively” for data encryption or certificates related to keys that are not subject to Law 59/2003 on Electronic Signatures.

Notes on the centralised key management system:

This document assigns responsibility for safekeeping users' private keys, in a centralised key management system, to the organisations that store the device on which these keys are stored.

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 Filing the private key

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

Subscribers can store keys delivered on software for the certificate duration period at least, but must then 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 will also keep 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 creation of keys procedure. 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 will be 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 signing system is implemented, the system generates the user keys on a centralised cryptographic device from which they cannot be exported.

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 CA's keys are activated via an *m out of n* process. See section 6.3.1

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

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

Camerfirma keeps minutes on CA private key management processes.

Notes on the centralised key management system:

If a centralised signing system is implemented, the subscriber receives a unique, secret activation key which will allow him/her to activate the key remotely in the same way as a local key store. For this purpose the subscriber must have installed the Cryptographic Server software in the device from which the key will be activated.

6.3.7 Private key deactivation method

The subscriber's private key will be 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.

Camerfirma keeps minutes on CA private key management processes.

6.3.8 Private key destruction method

Before the keys are destroyed, a revocation of the certificate of linked public keys will be issued.

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

Backups will be 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

In accordance with article 20 f) of Law 59/2003 on Electronic Signatures, the CA will keep 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. Secure signature creation device life cycle.

Certificates for CAs belonging to the **JCC or JCS** hierarchies store the subscriber's keys in a secure signature creation device **(Hardware)** or a secure signature creation data storage device **(software)**. This situation is specified on the certificate.

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.

Software devices are also used in secure server certificates where the keys are generated 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 will be described on Camerfirma's web site
http://www.bit4id.com/espanol/descargas_camerfirma.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.

6.6. 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. Antivirus settings.
8. Network traffic requirements

6.6.1 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.

6.6.2 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.

6.7. Life cycle security controls

6.7.1 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

6.7.2 Security management controls

6.7.2.1 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.

6.7.2.2 Data and asset classification and management

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

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

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

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

Reference documentation: **IN-2005-02-04-Política de Seguridad.**

6.7.2.3 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 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-Asset Classification and Inventory

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 of the responses and an economic evaluation of the incident solution.

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

Operating procedures and responsibilities

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

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

6.7.2.4 Access system management

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

Reference documentation: **IN-2011-04-10-CONTROL_DE_ACCESOS_A_RED.**

In particular:

General CA

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

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

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

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

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

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

Creating the certificate

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

Revocation management

Revocation will take place via strict card-based authentication of an authorised administrator's applications. The log systems will generate evidence that guarantee 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.

6.7.2.5 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 will be 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 will be carried out by at least two trustworthy employees.

6.7.3 Life cycle security evaluation

Not stipulated

6.8. 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-CONTROL_DE_ACCESOS_A_RED.**

6.9. 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**

6.10. Cryptographic module engineering controls

All 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 in accordance with this policy comply with standard X.509 version 3, RFC 3739 and ETSI 101 867 "Qualified Certificate Profile".

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 public key algorithm object identifier is
1. 2. 840. 113549. 1. 1. 5 SHA-1 with RSA Encryption

The public key algorithm object identifier is
1.2.840.113549.1.1.1 rsaEncryption

7.1.4 Name restrictions

The names contained in the certificates are restricted to 'Distinguished Names' X.500, which are unique and unambiguous

7.1.5 Certification Policy (OID) object identifier

Every certificate has a policy identifier in accordance with the following model:

1.3.6.1.4.1.17326.10.X.Y.Z. For certificates issued by Camerfirma Public Administrations the following OID has been designated at the request of policies defined by the State Administration 1.3.6.1.4.1.17326.1.X.Y.Z

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

For Root and Intermediate Certification authorities, a policy OID has also been defined with the prefix 1.3.6.1.4.1.17326.10. The OID in certificate authorities limit the set of policies that are found along the certification chain. In our case, the OID 1.3.6.1.4.1.17326.10. must appear throughout the entire chain.

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.

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.

7.3. OCSP profile

In accordance with the RFC 2560 standard.

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 specifying changes.

This CPS will be amended when any significant changes are made to certificate management, for any type of certificate to which it applies. Two-yearly reviews will take place should no changes have been made in that time. These reviews will be 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 will be published immediately on Camerfirma's web site

http://www.camerfirma.com/camerfirmaPublic/index/Area-Usuario/Politicas-y-DPC.html

This document contains a section on changes and versions, specifying the changes that occurred since it was created and the dates of those changes.

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 will be available at:
http://www.camerfirma.com/camerfirmaPublic/index/Area-Usuario/Politicas-y-DPC.html

8.4. CPS approval procedures

The publication of reviewed versions of this CPS must be approved by Camerfirma Management.