CERTIFICATION PRACTICES STATEMENT DIGITAL CERTIFICATES AC CAMERFIRMA SA

Version 3.3.5

Language: **English**

FRANCE MARIE SYLVIA VIDAL LECA

Firmado digitalmente por FRANCE MARIE SYLVIA VIDAL LECA
Fecha: 2020.06.11 12:06:46 +02'00'

RAMIRO MUÑOZ MUÑOZ

Firmado digitalmente por RAMIRO MUÑOZ MUÑOZ
Fecha: 2020.06.11 13:03:05 +02'00'

Table of Contents

1. INTRODUCTION

1.1. Overview

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

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

Certification Practice Statement (CPS) is defined as a set of practices adopted by a Certification Authority for issuing certificates. It usually contains detailed information about its certificate security, support, administration and issue system, as well as the trust relationship between the Signatory/Subscriber or Trusting Third Party and the Certification Authority. These may be completely comprehensible and robust documents which provide an accurate description of the services offered, detailed certificate life cycle management procedures, and so on.

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

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

In summary, a Policy defines “what” security requirements are required for issuing certificates. The Certification Practice Statement tells us “how” the security requirements established in the Policy are fulfilled.

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

- RCF 3647 – *Internet X. 509 Public Key Infrastructure Certificate Policy*, de IETF,
- RFC 3739 3039 Del IETF Internet X.509 Public Key Infrastructure: Qualified Certificates Profile.
- RFC 5280, RFC 3280: Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL).
- RFC 6960 Online Certificate Status Protocol - OCSP
- ETSI TS 101 456 V1.2.1 Policy requirements for certification authorities issuing qualified certificate
- ETSI TS 102 042 V1.1.1 Policy requirements for certification authorities issuing public key certificate

- These practices are aligned with the requirements set out in the *Baseline Requirements for the Issue and Management of Publicly-Trusted Certificates* prepared by the CA/B Forum http://www.cabforum.org in its version 1.6.5

In the event that of any inconsistency between this document and the *Baseline Requirements,* the *Baseline Requirements* shall take precedence over this document.

Additionally, in the requirements established in the certification policies to which this CPS refers. The recommendations in the technical document *Security CWA 14167-1 Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1: System Security Requirements* have also been taken into consideration.

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

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

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

1.2. Document Name and Identification

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

1.3. PKI participants

1.3.1 Certification authorities

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

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

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

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

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

1.3.2 Registration authorities

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

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

- Chambers RA: Those managed directly or under the control of a Spanish Chamber of Commerce, Industry and Navigation.
- Corporate RA: Managed by a public organization or a private entity for distributing certificates to its employees. It will be controlled by a Cameral AR when we talk about the AC "Camerfirma Certificados Camerales".
- Remote RA: A registration authority managed in a remote location that communicates with the platform through the AC Camerfirma - STATUS management platform integration layer.
- PVP. Point of Physical Verification that always depends on an RA. Its main mission is to provide evidence of the applicant's physical presence and deliver the documentation to the RA, which is validated in accordance with applicable policy for processing the application for issuing the certificate. For these functions, the PVPs are not subject to training, but may be subject to specific controls.

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

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

For the Chambers of Commerce Root Hierarchy:

- The Certification Authority.
- The Chambers of Commerce, Industry and Navigation, or the entities appointed by them. The registration process can be carried out on behalf of the different delegated entities:
- The Business Registration Authorities (Business RA), as entities delegated by a RA, to which they are contractually bound, in order to carry out the complete registrations of Signatories/Subscribers within a certain organization or demarcation. In general, the operators of the said Business RAs shall solely manage the applications and the certificates in the scope of their organization or demarcation, unless it is determined in another way by the RA that they depend on. For example, a corporation's employees, members of a corporate group, members of a professional body.
- The Public Administration, in the case of certificates issued under the AC Camerfirma Public Administrations.
- Any RA can delegate, in the Physical Verification Point (PVPs), the certificate-holder's on-site verification function and the receipt of documentation and, if applicable, the compiling of documentation and verification of its suitability as well as the delivery of material. In view of the fact that they do not have the ability to register, they are contractually bound with an RA by means of a contract that is provided by Camerfirma. Based on the documentation supplied by the PVP, the RA operator checks the documentation and, if applicable the CA issues the certificate with no need to carry out a new on-site verification. The contract defines the functions delegated by the RA in the PVP.

For the Chambersign Hierarchy.

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

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

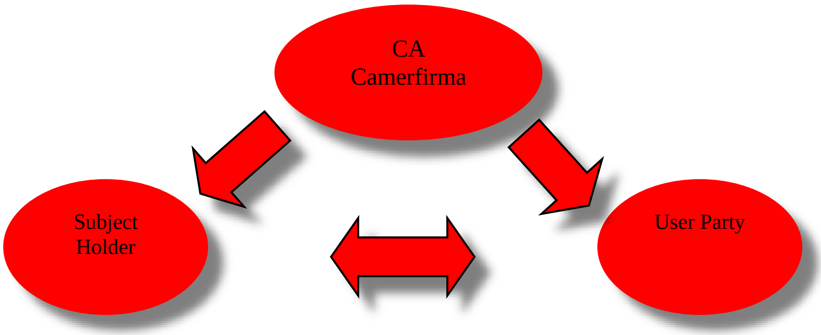
In the issuance of Secure Server certificates the delegation of domain validation to an external RA IS NOT allowed in any case.

1.3.3 Subscribers

We understand the Signatory / Subscriber to the certificate holder when this is a natural or legal person and is described in the CN field of the certificate. When issued in the name of a hardware device or computer application, the person or legal entity requesting the certificate issued shall be considered the signatory / Subscriber.

1.3.4 Relying parties

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



1.3.5 Other participants

1.3.5.1 Intermediate or Subordinate Certification Authority.

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

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

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

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

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

1.3.5.2 Accreditation Entity or Supervisory Body.

The accreditation body will be the corresponding managing body that admits, accredits and supervises the certification bodies. This task falls to the Ministry of Industry, Tourism and Trade of the Government of Spain, which is the competent authority depending on the Spanish Member State of the European Economic Area, in accordance with the legislation issued in compliance with Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

The SubCAs developed by Camerfirma may be subject to legal frameworks of different countries or regions, with the Accreditation entity falling, in these cases, into the corresponding national bodies.

- Spain: Ministerio de Industria, Energía y Turismo. http://www.minetur.gob.es
- Andorra: Ministeri d’Economia y Territori del Govern d’Andorra

1.3.5.3 Trusted Service Provider (TSP).

We understand under this CPS, a PSC as that entity, trusted third party, that provides the specific services related to the life cycle of the certificates and that can directly or indirectly manage one or more Certification Authorities and associated services such as issue of time stamps, provision of signature devices or validation services.

AC Camerfirma issues SubCA certificates to third parties for accreditation within and outside of the Spanish legal framework, and these third parties may be considered PSC in those countries before their national Accreditation entities.

1.3.5.4 Entity/Organization.

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

And so

- In the case of the certificate of persona física, de empleado público de vinculación, de Certificat d´actuació de PERSONA FÍSICA al servei de l´ADMINISTRACIÓ, de Certificat d’actuació de PERSONA FÍSICA al servei d’una ORGANITZACIÓ, Certificat d’actuació de PERSONA FÍSICA PROFESSIONAL COL·LEGIAT, the Entity is linked to the Signatory/Subscriber by means of a mercantile, labour, collegiate relation, etc.

- In the case of Representante, Certificat d’actuació de REPRESENTANT PERSONA JURÍDICA, the Entity is represented with broad powers by the Signatory/Subscriber.

- In case of certificado de Representante de Entidad sin Personalidad Jurídica para trámites con las AAPP en QSCD, the Entity is represented with powers by the Subscriber/Signatory for procedures with the Public Administrations.

- In case of certificado de Representante de Entidad sin Personalidad Jurídica para trámites con las AAPP, the Entity is represented with powers by the Signatory / Subscriber for procedures with the AAPP.

- In case of certificado de Apoderamiento Especial, the Entity is represented for certain procedures by the Signatory/Subscriber.

- In case of certificado de Facturación electrónica, the Entity authorizes the Signatory/Subscriber to perform the electronic invoicing of the same.

- In the case of Servidor Seguro/Sello electrónico/Cualificado de Sello Electrónico en QSCD/Cualificado de Sello Electrónico, Sede electrónica, Certificat d'actuació de SEGELL D'EMPRESA (Persona Jurídica), Certificat d'actuació d'Administració, Òrgan o Entitat de Dret Públic, the Entity is the owner of the Internet domain or the application for which the certificate has been requested.

As a general rule, the Entity is identified within the certificate in the organization field (O) and its fiscal identifier in a field owner of the certificate. For more information see section 3.1.1.

1.3.5.5 Applicant

Applicant will be understood as the individual who makes the request to issue the Certificate to the PSC, either directly or through an authorized representative.
They can be applicants:

- The person who will be the future signer of the certificate.
- A representative of the organization under which the certificate will be issued.
- A person authorized by the future subscriber/signer of the certificate.
- A person authorized by the Registration Authority.
- A person authorized by the Certification Authority.

1.3.5.6 Certificate Holder/Key Holder

For certificates issued to individuals, this CPS considers the certificate holder (the signatory/subscriber) responsible.

For certificates issued to legal entities, this CPS considers the physical person making the request responsible (the applicant) who must be identified within the certificate, even if the request is made through a third party, when the latter has knowledge of the existence of the certificate.

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

1.3.5.7 End User

End users are the people who obtain and use personal, entity, device and object certificates issued by the Certification Entities, and, specifically, we can distinguish the following end users:

- Certificate applicants.
- Subscribers or certificate holders.
- Key holders.
- The verifiers of signatures and certificates.

1.3.5.8 *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 organizing them in the different CAs.

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

Camerfirma manages two hierarchical structures:

- Chambers of Commerce Root.
- Global Chambersign Root.

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

1.3.5.8.1 *Issuing test certificates*

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

Name of the entity	[TEST ONLY] ENTITY
Entity Tax ID No.	R05999990
Entity address (street/number)	ADDRESS
Post code	5001
Contact telephone	902361207
Name	JUAN
First Surname	CÁMARA
Second Surname	SPANISH
National ID No.	00000000T

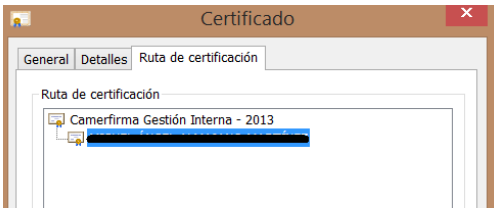
In cases where the approval, evaluation process... Requires a test certificate to be issued with real data, the process is carried out after the signing of a confidentiality agreement with the entity responsible for overseeing approval or evaluation tasks. The data is specified by each customer, but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

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

1.3.5.8.2 Camerfirma Internal Management Hierarchy.

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

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



Ruta de certificación

Camerfirma Gestión Interna - 2013

[redacted]

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

1.3.5.9 Chambers of Commerce Root Hierarchy.

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.

The characteristics of this hierarchy are summarised below:

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

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

Chambers of Commerce Root	
AC Camerfirma Express Corporate Server	1.3.6.1.4.1.17326.10.11.1
AC Camerfirma Certificados Camerales	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
Legal entities.	1.3.6.1.4.1.17326.10.9.4
Special Power of Attorney.	1.3.6.1.4.1.17326.10.9.5
Representative Certificate of Legal Person for paperwork with the AAPP	1.3.6.1.4.1.17326.10.16.1.3.2
Certificado de Cifrado (Software)	1.3.6.1.4.1.17326.10.9.6
Certificado de Factura electrónica	1.3.6.1.4.1.17326.10.9.7
AC CAMERFIRMA AAPP	1.3.6.1.4.1.17326.1.3.1

Electronic office, high-level.	1.3.6.1.4.1.17326.1.3.3.1
Electronic office, mid-level.	1.3.6.1.4.1.17326.1.3.3.2
Electronic Seal for Automated Procedures, high-level.	1.3.6.1.4.1.17326.1.3.4.1
Electronic Seal for Automated Procedures, mid-level.	1.3.6.1.4.1.17326.1.3.4.2
Public Employee, high-level, signature.	1.3.6.1.4.1.17326.1.3.4.3
Public Employee, high-level, authentication.	1.3.6.1.4.1.17326.1.3.4.4
OCSP Responder	1.3.6.1.4.1.17326.10.9.8

1.3.5.9.1 AC Camerfirma Express Corporate Server.

It is an intermediate CA that issued digital certificates whose holders were machines or applications.

All the certificates it issued expired before this CPS was drafted.

1.3.5.9.2 AC Camerfirma Chambers 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, pursuant to the criteria established in Law 59/2003, 19 December, on electronic signatures, the functions of which are described below.

The final certificates are intended for:

1.3.5.9.2.1 Natural persons with a business relationship with an Entity.

1.3.5.9.2.1.1 Contractual relationship with Entity.

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

1.3.5.9.2.1.2 Powers of Representation.

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

1.3.5.9.2.1.3 Special Power of Attorney.

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

1.3.5.9.2.1.4 Certificate of Representative of Legal Entity for procedures with the Public Administrations

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

1.3.5.9.2.1.5 Certificate of Representative of Entity Without Legal Personality for procedures with the AAPP

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

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

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

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

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

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

1.3.5.9.2.2.1 *Electronic invoicing.*

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

1.3.5.9.2.2.2 *Encryption.*

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

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

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

1.3.5.9.3 AC Camerfirma AAPP.

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

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

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

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

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

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

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

1.3.5.10 Hierarchy Global Chambersign ROOT.

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

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

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

The main characteristics of this hierarchy are:

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

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

AC Camerfirma	AnyPolicy
RACER	AnyPolicy
Certificado de Persona Física de Vinculación Pertenencia	1.3.6.1.4.1.17326.10.8.2
Certificado de Persona Física de Vinculación Representación	1.3.6.1.4.1.17326.10.8.3
Certificado de persona jurídica	1.3.6.1.4.1.17326.10.8.4
Certificado de Persona Física Ciudadano Emprendedor	1.3.6.1.4.1.17326.10.8.6
Certificado de Persona Física de Vinculación Factura Electrónica	1.3.6.1.4.1.17326.10.8.7
Certificado de Persona Física de Vinculación Apoderado	1.3.6.1.4.1.17326.10.8.8
PERSONA FÍSICA en DSCF – SIGNATURA	2.16.20.2.1.3.1.1.3
PERSONA FÍSICA en DSCF – IDENTITAT	2.16.20.2.1.3.1.1.1
PERSONA FÍSICA en programari	2.16.20.2.1.3.1.1.2
PERSONA FÍSICA PROFESSIONAL en DSCF – SIGNATURA	2.16.20.2.1.3.1.12.3

	PERSONA FÍSICA PROFESSIONAL en DSCF – IDENTITAT	2.16.20.2.1.3.1.12.1
	PERSONA FÍSICA PROFESSIONAL en programari	2.16.20.2.1.3.1.12.2
	PERSONA FÍSICA PROFESSIONAL COL·LEGIAT en DSCF – SIGNATURA	2.16.20.2.1.3.1.12.3
	PERSONA FÍSICA PROFESSIONAL COL·LEGIAT en DSCF – IDENTITAT	2.16.20.2.1.3.1.12.1
	PERSONA FÍSICA PROFESSIONAL COL·LEGIAT en DSCF – XIFRAT	2.16.20.2.1.3.1.11.1
	PERSONA FÍSICA PROFESSIONAL COL·LEGIAT en programari	2.16.20.2.1.3.1.12.2
	PERSONA FÍSICA al servei d’una ORGANITZACIÓ en DSCF – SIGNATURA	2.16.20.2.1.3.1.4.3
	PERSONA FÍSICA al servei d’una ORGANITZACIÓ en DSCF – IDENTITAT	2.16.20.2.1.3.1.4.1
	PERSONA FÍSICA al servei d’una ORGANITZACIÓ en programari	2.16.20.2.1.3.1.4.2
	PERSONA FÍSICA al servei de l´ADMINISTRACIÓ en DSCF – SIGNATURA	2.16.20.2.1.3.1.5.3
	PERSONA FÍSICA al servei de l´ADMINISTRACIÓ en DSCF – IDENTITAT	2.16.20.2.1.3.1.5.1
	PERSONA FÍSICA al servei de l´ADMINISTRACIÓ en DSCF – XIFRAT	2.16.20.2.1.3.1.11.1
	PERSONA FÍSICA al servei de l’ADMINISTRACIÓ en programari	2.16.20.2.1.3.1.5.2
	SEGELL D’EMPRESA (Persona Jurídica) en HSM - Segell Electrònic	2.16.20.2.1.3.1.2.3
	SEGELL D’EMPRESA (Persona Jurídica) en HSM – IDENTITAT	2.16.20.2.1.3.1.2.1
	SEGELL D’EMPRESA (Persona Jurídica) en programari	2.16.20.2.1.3.1.2.2
	REPRESENTANT PERSONA JURÍDICA en HSM - Segell Electrònic	2.16.20.2.1.3.1.3.3
	REPRESENTANT PERSONA JURÍDICA en HSM – IDENTITAT	2.16.20.2.1.3.1.3.1
	REPRESENTANT PERSONA JURÍDICA en programari	2.16.20.2.1.3.1.3.2

Certificat d’actuació d’Administració, Òrgan o Entitat de Dret Públic en HSM	2.16.20.2.1.3.1.8.3
Certificat d’actuació d’Administració, Òrgan o Entitat de Dret Públic en programari	2.16.20.2.1.3.1.8.2
Entidad de Certificación de la Administración Pública Andorrana-19 (Andorra)	AnyPolicy
PERSONA FÍSICA en DSCF – SIGNATURA	2.16.20.2.1.3.1.1.3
PERSONA FÍSICA en DSCF – IDENTITAT	2.16.20.2.1.3.1.1.1
PERSONA FÍSICA en programari	2.16.20.2.1.3.1.1.2
PERSONA FÍSICA PROFESSIONAL en DSCF – SIGNATURA	2.16.20.2.1.3.1.12.3
PERSONA FÍSICA PROFESSIONAL en DSCF – IDENTITAT	2.16.20.2.1.3.1.12.1
PERSONA FÍSICA PROFESSIONAL en programari	2.16.20.2.1.3.1.12.2
PERSONA FÍSICA PROFESSIONAL COL·LEGIAT en DSCF – SIGNATURA	2.16.20.2.1.3.1.12.3
PERSONA FÍSICA PROFESSIONAL COL·LEGIAT en DSCF – IDENTITAT	2.16.20.2.1.3.1.12.1
PERSONA FÍSICA PROFESSIONAL COL·LEGIAT en DSCF – XIFRAT	2.16.20.2.1.3.1.11.1
PERSONA FÍSICA PROFESSIONAL COL·LEGIAT en programari	2.16.20.2.1.3.1.12.2
PERSONA FÍSICA al servei d’una ORGANITZACIÓ en DSCF – SIGNATURA	2.16.20.2.1.3.1.4.3
PERSONA FÍSICA al servei d’una ORGANITZACIÓ en DSCF – IDENTITAT	2.16.20.2.1.3.1.4.1
PERSONA FÍSICA al servei d’una ORGANITZACIÓ en programari	2.16.20.2.1.3.1.4.2
PERSONA FÍSICA al servei de l´ADMINISTRACIÓ en DSCF – SIGNATURA	2.16.20.2.1.3.1.5.3
PERSONA FÍSICA al servei de l´ADMINISTRACIÓ en DSCF – IDENTITAT	2.16.20.2.1.3.1.5.1
PERSONA FÍSICA al servei de l´ADMINISTRACIÓ en DSCF – XIFRAT	2.16.20.2.1.3.1.11.1
PERSONA FÍSICA al servei de l’ADMINISTRACIÓ en programari	2.16.20.2.1.3.1.5.2
SEGELL D’EMPRESA (Persona Jurídica) en HSM - Segell Electrònic	2.16.20.2.1.3.1.2.3
SEGELL D’EMPRESA (Persona Jurídica) en HSM – IDENTITAT	2.16.20.2.1.3.1.2.1
SEGELL D’EMPRESA (Persona Jurídica) en programari	2.16.20.2.1.3.1.2.2

REPRESENTANT PERSONA JURÍDICA en HSM - Segell Electrònic	2.16.20.2.1.3.1.3.3
REPRESENTANT PERSONA JURÍDICA en HSM – IDENTITAT	2.16.20.2.1.3.1.3.1
REPRESENTANT PERSONA JURÍDICA en programari	2.16.20.2.1.3.1.3.2
Certificat d’actuació d’Administració, Òrgan o Entitat de Dret Públic en HSM	2.16.20.2.1.3.1.8.3
Certificat d’actuació d’Administració, Òrgan o Entitat de Dret Públic en programari	2.16.20.2.1.3.1.8.2

1.3.5.10.1 AC Camerfirma

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

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

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

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

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

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

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

1.3.5.10.2 Certification Entity of the Andorra Public Administration.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1.4. Scope of Application and Certificate usage

This CPS fulfils the Certification Policies described in section 0 of this CPS.

1.4.1 Appropriate certificate uses

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

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

- Authentication based on certificates X.509v3.
- Electronic signature, advanced or recognised, based on certificates X.509v3.
- Asymmetric or mixed encryption, based on certificates X.509v3.

1.4.2 Prohibited certificate uses

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

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

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

Camerfirma does not have access to the data for which a certificate is used. Therefore, due to this technical impossibility of being able to access the message content, Camerfirma cannot issue any appraisal regarding this content, and the signatory is consequently responsible for the content linked to the use of the certificate. The signatory is also responsible for the consequences of any use of this data in breach of the limitations and terms and conditions established in the Certification Policies applicable to each Certificate, the CPS and the contracts the CAs sign with the Signatories, as well as any misuse thereof pursuant to this paragraph or which could be interpreted as such by virtue of current law.

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

1.5. Policy administration

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

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

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

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

1.5.1 Organization administering the document

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

1.5.2 Contact person

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

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

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

1.5.3 Person determining CPS suitability for the policy

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

1.5.4 CPS approval procedures

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

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

1.6. Definitions and Acronyms

1.6.1 Acronyms

CA	Certification Authority
CPS	Certification Practice Statement.
CRL	Certificate Revocation List. List of revoked certificates
CSR	Certificate Signing Request.
DES	Data Encryption Standard. Standard for encrypting data
DN	Distinguished Name. Distinguished name in the digital certificate
DSA	Digital Signature Algorithm. The signature's algorithm standard
FIPS	Federal Information Processing Standard Publication
IETF	Internet Engineering Task Force
ISO	International Standards Organization
ITU	International Telecommunications Union.
LDAP	Lightweight Directory Access Protocol. Protocol for directory access
OCSP	On-line Certificate Status Protocol. Protocol for accessing the status of certificates
OID	Object Identifier.
PA	Policy Authority.
PC	Certification Policy
PIN	Personal Identification Number.
PKI	Public Key Infrastructure.

RA Registration Authority

RSA Rivest-Shamir-Adleman. Type of encryption algorithm

SHA Secure Hash Algorithm.

SSCD Secure Signature Creation Device

SSCDSD Secure Signature Creation Data Storage Device

SSL Secure Sockets Layer. A protocol designed by Netscape that has become standard on the Internet. It allows the transmission of encrypted information between a browser and a server.

TCP/IP Transmission Control. *Protocol/Internet Protocol*. System of protocols, as defined in the IETF framework. The TCP protocol is used to split source information into packets and then recompile it on arrival. The IP protocol is responsible for correctly directing the information to the recipient.

1.6.2 Definitions

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

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

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

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

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

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

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

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

Digital signature

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

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

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

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

Entity

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

Key pair

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

OID

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

PKI

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

Policy authority

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

Private key

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

Public key

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

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

Registration Authority

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

SCDSD

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

SSCD

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

Subject/Signatory

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

User Party

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

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. Repositories

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

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

Policy and certification practice repository. These services are available to the public on AC Camerfirma's website at https://www.camerfirma.com/politicas-de-certificacion-ac-camerfirma/.

Camerfirma publishes the issued certificates, revocation lists, and certification policies and practices at no cost at https://www.camerfirma.com/area-de-usuario/consulta-de-certificados/.

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

2.2. Publication of certification information

Camerfirma generally publishes the following information in its repository:

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

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

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

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

2.2.1 Certification Policies and Practices.

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

Subordinate CA certification policies are also published or referenced on AC Camerfirma's website. https://www.camerfirma.com/politicas-de-certificacion-ac-camerfirma/

2.2.2 Terms and conditions.

Camerfirma makes available to users, the terms and conditions of service, in its policies and practices of certification. The Subject/Signer receives information of the terms and conditions in the process of issuing the certificate, either through the form of the physical contract or through the process of electronic acceptance of conditions of service as an indispensable step to proceed with the request.

When the subject/signatory accepts the terms and conditions on paper it must be done through a handwritten signature. In the case that it is accepted in electronic format, it is done by accepting the terms and conditions in the application form, in accordance with the provisions of current regulations on contracting by electronic means.

2.2.3 Distribution of the certificates.

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

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

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

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

2.3. Time or frequency of publication

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

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

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

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

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

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

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

2.4. Access controls on repositories

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

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

Camerfirma uses reliable systems for the repository, in such a way that:

The authenticity of the certificates can be checked. The certificate itself signed by the certification authority guarantees its authenticity.

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

3. IDENTIFICATION AND AUTHENTICATION

3.1. Naming

3.1.1 Types of names

The Signatory/Subscriber is described in the certificates by a distinguished name (DN, distinguished name, Subject) pursuant to the X.501 standard. The DN field descriptions are shown in each of the certificate profile documents. Similarly, it includes a "Common Name" component (CN =).

The profile sheets can be requested through the customer support service of AC Camerfirma 902 361 207 or through the application https://www.camerfirma.com/ayuda/soporte/ .

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

- In certificates corresponding to natural persons the identification of the signatory is formed by their name and surname(s), in addition to their tax identification code.
- Certificates corresponding to legal entities shall be identified by means of their corporate or business name and tax identification code.
- The structure for the SubCA, OCSP certificates includes, at least:
  - A descriptive name that identifies the Certification Authority (CN)
  - The legal entity responsible for the keys (O)
  - The tax identification number of the organization responsible for the keys (SN)
  - The country where the corporate activity of the organization responsible for the keys is undertaken. (C)
- The ROOT certificates have a descriptive name that identifies the Certification Authority and in the field (O) the name of the organization responsible for the Certification Authority

3.1.2 Need for names to be meaningful

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

3.1.3 Anonymity or pseudonymity of subscribers

Not available.

3.1.4 Rules for interpreting various name forms

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

3.1.5 Uniqueness of names

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

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

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

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

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

3.1.6 Recognition, authentication and role of trademarks

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

3.1.6.1 Name dispute resolution procedure

Camerfirma has no responsibility in the case of resolution of name disputes.

In any case, the assignment of names will be made based on their order of entry.

Camerfirma does not arbitrate this type of disputes that must be resolved directly by the parties.

Camerfirma in any case complies with the provisions of section 9.13 of this CPS.

3.2. Initial identity validation

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

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

3.2.1 Method to prove possession of private key

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

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

a) Keys created by Camerfirma.

   In Software: Delivered to the Subject/Signer by hand or by mail through protected files using the PKCS#12 Standard. The security of the process is guaranteed because the access code to the PKCS#12 file, which enables its installation in the applications, is delivered by a different means than the one used to receive the file.

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

   In remote centralized storage: Camerfirma uses a remote key storage system, allowing the Subject/Signer to access the key from different devices. The keys are stored in a FIPS-140-2 level 3 certified HSM device (included in the list of devices notified by Member States as Secure Signature Creation Qualified Devices https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds) ensuring unique control of the key by the Subject/Signatory. This type of storage is not performed for SSL/TLS secure server certificates

b) Keys created by the Signatory.

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

3.2.2 Authentication of organization identity

3.2.2.1 Identity

Before a certificate issued to a legal person or a natural person with the capacity to bind an entity can be issued and delivered, it is necessary to authenticate the data relating to the establishment and legal personality of the entity.

For these certificates, the identification of the entity is required in all cases, for which the RA will require the relevant documentation according to the type of entity. The relevant documentation can be found on the Camerfirma website in the information section of the corresponding certificate.

In the case of entities outside Spanish territory, the documentation to be provided will be that from the Official Register of the corresponding country, duly apostilled and with a sworn translation into Spanish indicating the existence of the entity in that country.

In addition, it is checked:

- That the data or documents provided are not more than 1 year old.
- That the legal existence of the organization is at least 1 year old.
- That they are not companies that have been eradicated in countries where there is a government ban on doing business or are on a blacklist of entities managed by the provider.

In Public Administrations: Documentation accrediting the existence of the public administration, body or entity under public law is not required, given that this identity forms part of the corporate scope of the General State Administration or other State Public Administrations.

3.2.2.2 Trademarks

See 3.1.6

3.2.2.3 Country Verification

See 3.2.2.1

3.2.2.4 Validation of domain authorization or control

See 3.2.5.1

3.2.2.5 Authentication of an IP address

Not available.

3.2.2.6 Wildcard Domain Validation

Not available.

3.2.2.7 Accuracy of data sources

See 3.2.2.1

3.2.2.8 CAA

Not available.

3.2.3 Authentication of individual identity

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

- National Identification Document.
- Residency card.
- Passport.
- ID document with Hague Apostille (and official translation if it’s necessary) for foreign citizens.

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

Physical attendance is not required for these certificates in the cases established in Law 59/2003 or European regulations directly applicable in Spain.

The documentation necessary to issue a certificate is published at: http://www.camerfirma.com/index/buscador-documentos.php

Control over the email address incorporated in the certificate request is checked by communicating a random value that will be required at the time of the generation and download of the certificate.

3.2.4 Non-verified subscriber information

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

3.2.5 Validation of authority

3.2.5.1 Proof of relationship

Type of certificate	Documentation
Certificado de representante (AC Camerfirma Certificados Camerales) Certificado de apoderado (AC Camerfirma Certificados Camerales) Certificado de persona jurídica (AC Camerfirma Certificados Camerales) Certificado de representante de Persona Jurídica (o de Entidad sin Personalidad Jurídica) para trámites con las AAPP Certificado de Persona Física de Vinculación Representación (RACER) Certificado de persona jurídica (RACER) Certificado de Persona Física de Vinculación Apoderado (RACER)	Evidence of the Subject/Signatory's capacity to represent the entity, by providing documentation demonstrating his/her powers of representation according to the type of entity. This information is published in the RA's Operating Manuals and on Camerfirma's website.

Type of certificate	Documentation
Certificado de pertenencia a empresa (AC Camerfirma Certificados Camerales) Certificado de Cifrado (Software) (AC Camerfirma Certificados Camerales) Certificado de Factura electrónica (AC Camerfirma Certificados Camerales) Certificado de Persona Física de Vinculación Pertenencia (RACER) Certificado de Persona Física Ciudadano Emprendedor (RACER) Certificado de Persona Física de Vinculación Factura Electrónica (RACER)	In general, authorization signed by a legal representative or general proxy of the entity that accredits the link between the Applicant and the Entity
Certificado reconocido de sello electronico de Administracion, organo o entidad de derecho publico, nivel alto (AC CAMERFIRMA AAPP) Certificado reconocido de sello electronico de Administracion, organo o entidad de derecho publico, nivel medio (AC CAMERFIRMA AAPP) Certificado reconocido de empleado publico, nivel alto, firma (AC CAMERFIRMA AAPP) Certificado reconocido de empleado publico, nivel alto, autenticación (AC CAMERFIRMA AAPP) Certificado reconocido de empleado publico, nivel alto, cifrado (AC CAMERFIRMA AAPP) Certificado reconocido de empleado publico, nivel medio (AC CAMERFIRMA AAPP)	Identity card of the person acting as a responsible person on behalf of the said public administration, body or entity under public law. The Applicant/Responsible Person will be identified before the RA with his/her ID and authorization of the responsible person where it is indicated that he/she is a public employee or appointment in the Official Gazette where the ID of this person is stated. Document that proves the ownership of the domain used in the applicant's mail by the entity associated with the electronic stamp certificate. The accepted documents can be: invoices or purchase contract.

Type of certificate	Documentation
Certificat d´actuació de PERSONA FÍSICA al servei de l´ADMINISTRACIÓ (Entidad de Certificación de la Administración Pública Andorrana + RACER) Certificat d'actuació de PERSONA FÍSICA (Entidad de Certificación de la Administración Pública Andorrana + RACER) Certificat d'actuació de PERSONA FÍSICA al servei d'una ORGANITZACIÓ (Entidad de Certificación de la Administración Pública Andorrana + RACER) Certificat d'actuació de PERSONA FÍSICA PROFESSIONAL COL·LEGIAT (Entidad de Certificación de la Administración Pública Andorrana + RACER) Certificat d'actuació de REPRESENTANT PERSONA JURÍDICA (Entidad de Certificación de la Administración Pública Andorrana + RACER)	E rticle 26.2 of Andorran Law 35/2014 of 27 November on electronic trust services provides that: "the qualified electronic trust service provider must reliably verify the identity and, where appropriate, any other specific attribution of the natural person to whom it issues the qualified electronic certificate, by displaying the public or private documents which it sufficiently certifies. This information should be verified by the qualified service provider or by a third party acting under the responsibility of the qualified service provider: i. Through the physical presence of this person, or ii. remotely, using other qualified electronic certificates issued by a qualified service provider". In addition, Article 26. 3 of the Andorran Law 35/2014 of 27 November on electronic trust services establishes that in the case of: "electronic certificates issued to natural persons but linked to an organization, entity, institution, company or other legal person, the provider of the trust service must prove, in addition to the identity of the applicant and the person identified in the electronic certificate, the data relating to the constitution and legal personality of the entity, or to the extension and validity of the powers or powers of representation of the applicant, by means of the public documents which it specifically accredits or by consulting the corresponding public register, which is the result of the data which must appear in the same".
Certificat d'actuació de SEGELL D'EMPRESA (Persona Jurídica) (Entidad de Certificación de la Administración Pública Andorrana + RACER) Certificat d'actuació d'Administració, Òrgan o Entitat de Dret Públic (Entidad de Certificación de la Administración Pública Andorrana + RACER)	Article 26.2 of Andorran Law 35/2014 of 27 November on electronic trust services states that: "the qualified electronic trust service provider shall verify the identity and, where appropriate, any other specific attribution of the legal person to which the qualified electronic certificate is issued, by showing public or private documents which provide sufficient proof. This information should be verified by the qualified service provider or by a third party acting under the responsibility of the qualified service provider: i. Through the physical presence of an authorised representative of that legal entity, or ii. remotely, using other qualified electronic certificates issued by a qualified service provider".

3.2.5.2 *Considerations in the identification of the user in cases of high position.*

AC Camerfirma uses special procedures for the identification of senior positions in companies and administration for the issuance of digital certificates. In these cases, a registry operator moves to the facilities of the organization to ensure the physical presence of the owner. For the relations between the holder and the organization represented in public administration, the publication of the positions in the official bulletins is usually used.

3.2.5.3 Considerations in the identification of users and linkage in the AAPP

There are aspects to consider regarding the registration authorities established in the public administration and operated by public employees, the latter being considered as notaries to guarantee the relationship between a public employee who requests the certificate and the body to which it is linked. In these cases, the collection of documentation that is part of the file can be simplified.

3.2.5.4 In RA operator certificates (natural person)

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

3.2.5.5 Special considerations for issuing certificates outside of Spanish territory

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

3.2.6 Criteria for interoperation

Camerfirma may provide services allowing for another CA to operate within, or interoperate with, its PKI. Such interoperation may include cross-certification, unilateral certification, or other forms of operation. Camerfirma reserves the right to provide interoperation services and to interoperate with other CAs; the terms and criteria of which are to be set forth in the applicable agreement.

3.3. Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

The identification of a renewal application is made through the certificate to be renewed. It will not be renewed if the certificate to renew has passed the 5 years since the last physical verification or equivalent process.

3.3.2 Identification and authentication for re-key after revocation

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

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

3.4. Identification and authentication for revocation request

The method for submitting revocation requests is established in section 4.9 of this document.

Camerfirma, or any of the entities that comprise it, may, on their own initiative, request the revocation of a certificate if they are aware or suspect that the subscriber’s private key has been compromised, or if they are aware of or suspect any other event that would make taking such action advisable.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

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

4.1. Certificate Application

4.1.1 Who can submit a certificate application

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

4.1.2 Enrollment process and responsibilities

4.1.2.1 Web forms.

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

https://www.camerfirma.com/

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

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

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

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

4.1.2.2 Batches.

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

4.1.2.3 Applications for final-entity certificates in HSM.

Applications for issuing certificates in HSM are made through a sales quotation at a sales area. https://www.camerfirma.com/camerfirma/localizacion.

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

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

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

- Records from key creation events indicating:

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

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

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

4.1.2.4 Applications via Web Services (WS) layer.

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

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

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

4.1.2.5 Cross certification request

Camerfirma allows under these practices the cross certification.

Camerfirma will evaluate the request and will demand the delivery of the corresponding audits that will allow to certify that the linked system fulfills technical, operative and legal regulations comparable before the generation of the certificate.

Camerfirma requests annual audit reviews from the client in order to maintain the cross certification.

4.2. Certificate application processing

4.2.1 Performing identification and authentication functions

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

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

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

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

Camerfirma use the following label in the DNS CAA record “issue” or “issuewild”: “camerfirma.com”

4.2.2 Approval or rejection of certificate applications

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

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

In requests via the WS layer, the request is authenticated at source and the issuance of the certificate by the platform is approved when the source and authentication are correct.

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

For SubCA certificates:
By commercial acceptance corresponding to a customer's request.

4.2.3 Time to process certificate applications

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

The requests presented by the PKI STATUS platform are validated once the supporting documentation associated to the certificate profile is checked. Camerfirma will proceed, whenever it is feasible, to eliminate the applications older than 1 year.

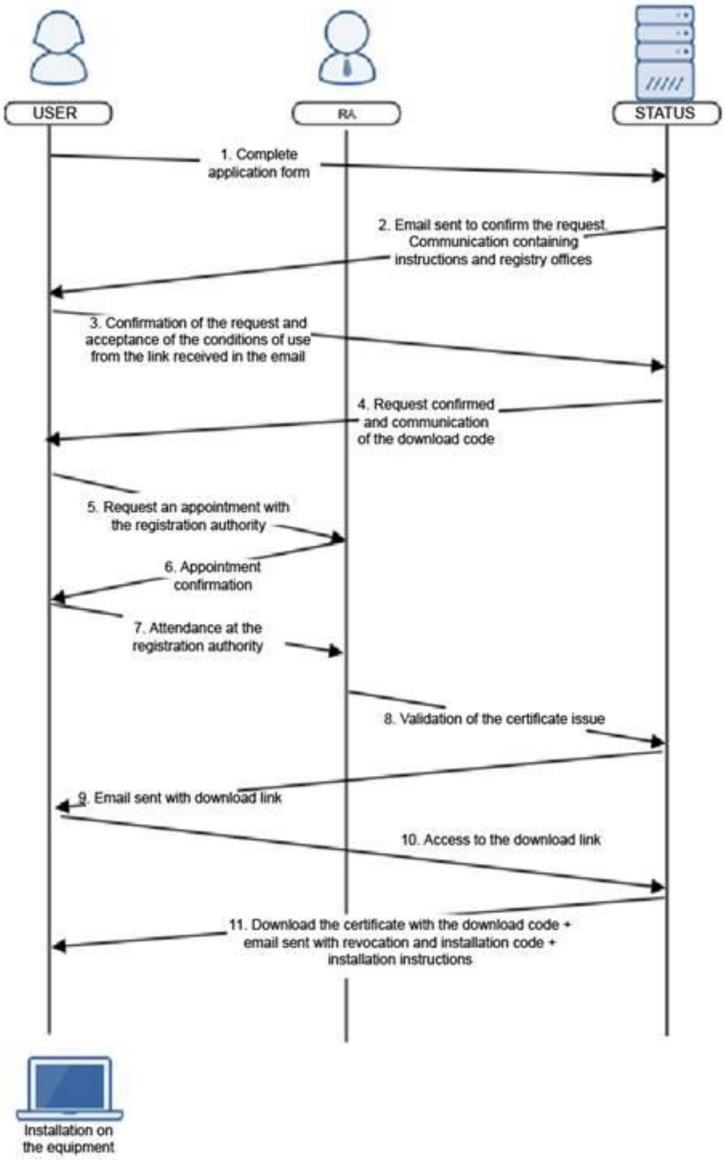
There are no stipulated deadlines for resolving a SubCA or cross-certification certificate request.

4.3. *Certificate issuance*

4.3.1 CA actions during certificate issuance

4.3.1.1 Certificates via Software:

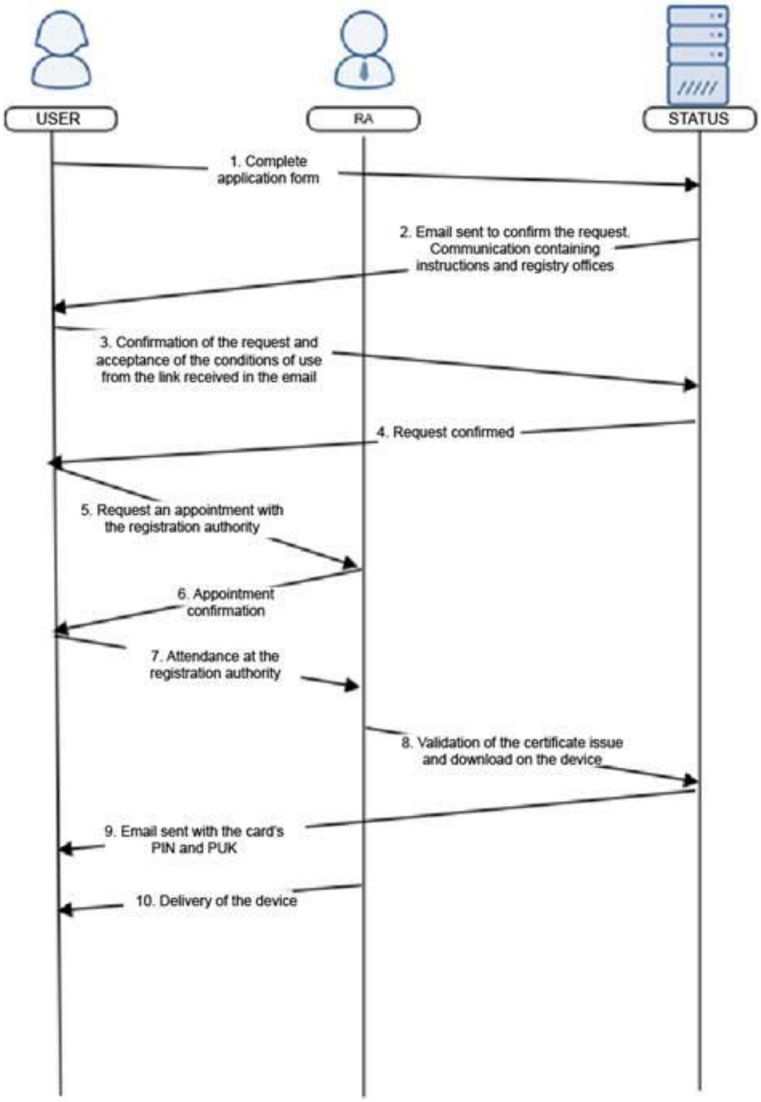
Once the application has been approved, the subscriber receives an e-mail with the approval notification, from which the certificate can be created and downloaded. The product code provided with the contract and an installation code sent in a separate email or via SMS together with a revocation code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


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

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

4.3.1.2 Certificates via HW (Secure Signature Creation Device):

4.3.1.2.1 Cryptographic Card or Token.


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

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

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

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

For the default cards (distributed by bit4id) the subscriber receives an e-mail in the associated account containing the access code to the cryptographic device and the unlocking code, as well as a renewal key. For other cards the PIN/PUK management is outside of the scope of this document.

4.3.1.3 **Applications via WS:**

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

4.3.2 Notification to subscriber by the CA of issuance of certificate

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

4.4. Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

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

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

4.4.2 Publication of the certificate by the CA

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

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

4.4.3 Notification of certificate issuance by the CA to other entities

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

In the case of SSL/TLS certificates as part of the “Certificate Transparency” process (https://www.certificate-transparency.org) a pre-certificate to a centralized registration service is sent prior to the final issue.

4.5. *Key pair and certificate usage*

4.5.1 Subscriber private key and certificate usage

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

CA	Key Usage	Extended Key Usage	Basic Constraints
Chambers of Commerce Root	critical, cRLSign, keyCertSign	-	critical,CA:true
AC Camerfirma Certificados Camerales	critical, cRLSign, keyCertSign	-	critical,CA:true
Certificado de pertenencia a empresa	critical, digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement	clientAuth, emailProtection	critical,CA:false
Certificado de representante	critical, digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement	clientAuth, emailProtection	critical,CA:false
Certificado de representante para trámites con las AAPP	critical, digitalSignature, contentCommitment, keyEncipherment	clientAuth, emailProtection	critical,CA:false
Certificado de persona jurídica	critical, digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement	clientAuth, emailProtection	critical,CA:false
Certificado de apoderado	critical, digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement	clientAuth, emailProtection	critical,CA:false
Certificado de Cifrado (Software)	critical, digitalSignature, contentCommitment, keyEncipherment	-	critical,CA:false
Certificado de Factura electrónica	critical, digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement	clientAuth, emailProtection	critical,CA:false
AC CAMERFIRMA AAPP	critical, cRLSign, keyCertSign	-	critical,CA:true
Certificado reconocido de sello electronico de Administracion, organo o entidad de derecho publico, nivel alto	critical, digitalSignature, contentCommitment, keyEncipherment, dataEncipherment	clientAuth, emailProtection	critical,CA:false
Certificado reconocido de sello electronico de Administracion, organo o entidad de derecho publico, nivel medio	critical, digitalSignature, contentCommitment, keyEncipherment, dataEncipherment	clientAuth, emailProtection	critical,CA:false
Certificado reconocido de empleado publico, nivel alto, firma	critical, nonRepudiation	-	critical,CA:false
Certificado reconocido de empleado publico, nivel alto, autenticacion.	critical, digitalSignature	clientAuth, emailProtection	critical,CA:false

Certificado reconocido de empleado publico, nivel alto, cifrado	critical, keyEncipherment, dataEncipherment	clientAuth, emailProtection	critical,CA:false
Certificado reconocido de empleado publico, nivel medio	critical, digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment	clientAuth, emailProtection	critical,CA:false
AC Camerfirma Express Corporate Server	critical, cRLSign, keyCertSign	-	critical,CA:true
Global Chambersign Root	critical, cRLSign, keyCertSign	-	critical,CA:true
AC Camerfirma	critical, cRLSign, keyCertSign	-	critical,CA:true
RACER	critical, cRLSign, keyCertSign	-	critical,CA:true
Certificado de Persona Física de Vinculación Pertenencia	critical, digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement	clientAuth, emailProtection	critical,CA:false
Certificado de Persona Física de Vinculación Representación	critical, digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement	clientAuth, emailProtection	critical,CA:false
Certificado de persona jurídica	critical, digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement	clientAuth, emailProtection	critical,CA:false
Certificado de Persona Física Ciudadano Emprendedor	critical, digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement	clientAuth, emailProtection	critical,CA:false
Certificado de Persona Física de Vinculación Factura Electrónica	critical, digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement	clientAuth, emailProtection	critical,CA:false
Certificado de Persona Física de Vinculación Apoderado	critical, digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA en DSCF – SIGNATURA	critical, nonRepudiation	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA en DSCF – IDENTITAT	critical, digitalSignature	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA en programari	critical, digitalSignature, keyEncipherment, nonRepudiation	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA PROFESSIONAL en DSCF – SIGNATURA	critical, nonRepudiation	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA PROFESSIONAL en DSCF – IDENTITAT	critical, digitalSignature	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA PROFESSIONAL en programari	critical, digitalSignature, keyEncipherment, nonRepudiation	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA PROFESSIONAL COL·LEGIAT en DSCF – SIGNATURA	critical, nonRepudiation	clientAuth, emailProtection	critical,CA:false

PERSONA FÍSICA PROFESSIONAL COL·LEGIAT en DSCF – IDENTITAT	critical, digitalSignature	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA PROFESSIONAL COL·LEGIAT en DSCF – XIFRAT	critical, keyEncipherment, dataEncipherment	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA PROFESSIONAL COL·LEGIAT en programari	critical, digitalSignature, keyEncipherment, nonRepudiation	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA al servei d’una ORGANITZACIÓ en DSCF – SIGNATURA	critical, nonRepudiation	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA al servei d’una ORGANITZACIÓ en DSCF – IDENTITAT	critical, digitalSignature	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA al servei d’una ORGANITZACIÓ en programari	critical, digitalSignature, keyEncipherment, nonRepudiation	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA al servei de l´ADMINISTRACIÓ en DSCF – SIGNATURA	critical, nonRepudiation	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA al servei de l´ADMINISTRACIÓ en DSCF – IDENTITAT	critical, digitalSignature	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA al servei de l´ADMINISTRACIÓ en DSCF – XIFRAT	critical, keyEncipherment, dataEncipherment	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA al servei de l’ADMINISTRACIÓ en programari	critical, digitalSignature, keyEncipherment, nonRepudiation	clientAuth, emailProtection	critical,CA:false
SEGELL D’EMPRESA (Persona Jurídica) en HSM - Segell Electrònic	critical, nonRepudiation	clientAuth, emailProtection	critical,CA:false
SEGELL D’EMPRESA (Persona Jurídica) en HSM – IDENTITAT	critical, digitalSignature	clientAuth, emailProtection	critical,CA:false
SEGELL D’EMPRESA (Persona Jurídica) en programari	critical, digitalSignature, keyEncipherment, dataEncipherment, nonRepudiation	clientAuth, emailProtection	critical,CA:false
REPRESENTANT PERSONA JURÍDICA en HSM - Segell Electrònic	critical, nonRepudiation	clientAuth, emailProtection	critical,CA:false
REPRESENTANT PERSONA JURÍDICA en HSM – IDENTITAT	critical, digitalSignature	clientAuth, emailProtection	critical,CA:false
REPRESENTANT PERSONA JURÍDICA en programari	critical, digitalSignature, keyEncipherment, nonRepudiation	clientAuth, emailProtection	critical,CA:false
Certificat d’actuació d’Administració, Òrgan o Entitat de Dret Públic en HSM	critical, digitalSignature, keyEncipherment, dataEncipherment, nonRepudiation	clientAuth, emailProtection	critical,CA:false
Certificat d’actuació d’Administració, Òrgan o Entitat de Dret Públic en programari	critical, digitalSignature, keyEncipherment, dataEncipherment, nonRepudiation	clientAuth, emailProtection	critical,CA:false
Entidad de Certificación de la Administración Pública Andorrana	critical, cRLSign, keyCertSign	-	critical,CA:true
Certificado de Persona Física de Vinculación Pertenencia	critical, digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement	clientAuth, emailProtection	critical,CA:false
Certificado de Persona Física de Vinculación Representación	critical, digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement	clientAuth, emailProtection	critical,CA:false
Certificado de persona jurídica	critical, digitalSignature,	clientAuth, emailProtection	critical,CA:false

	contentCommitment, keyEncipherment, dataEncipherment, keyAgreement		
Certificado de Persona Física Ciudadano Emprendedor	critical, digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement	clientAuth, emailProtection	critical,CA:false
Certificado de Persona Física de Vinculación Factura Electrónica	critical, digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement	clientAuth, emailProtection	critical,CA:false
Certificado de Persona Física de Vinculación Apoderado	critical, digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA en DSCF – SIGNATURA	critical, nonRepudiation	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA en DSCF – IDENTITAT	critical, digitalSignature	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA en programari	critical, digitalSignature, keyEncipherment, nonRepudiation	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA PROFESSIONAL en DSCF – SIGNATURA	critical, nonRepudiation	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA PROFESSIONAL en DSCF – IDENTITAT	critical, digitalSignature	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA PROFESSIONAL en programari	critical, digitalSignature, keyEncipherment, nonRepudiation	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA PROFESSIONAL COL·LEGIAT en DSCF – SIGNATURA	critical, nonRepudiation	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA PROFESSIONAL COL·LEGIAT en DSCF – IDENTITAT	critical, digitalSignature	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA PROFESSIONAL COL·LEGIAT en DSCF – XIFRAT	critical, keyEncipherment, dataEncipherment	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA PROFESSIONAL COL·LEGIAT en programari	critical, digitalSignature, keyEncipherment, nonRepudiation	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA al servei d'una ORGANITZACIÓ en DSCF – SIGNATURA	critical, nonRepudiation	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA al servei d'una ORGANITZACIÓ en DSCF – IDENTITAT	critical, digitalSignature	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA al servei d'una ORGANITZACIÓ en programari	critical, digitalSignature, keyEncipherment, nonRepudiation	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA al servei de l´ADMINISTRACIÓ en DSCF – SIGNATURA	critical, nonRepudiation	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA al servei de l´ADMINISTRACIÓ en DSCF – IDENTITAT	critical, digitalSignature	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA al servei de l´ADMINISTRACIÓ en DSCF – XIFRAT	critical, keyEncipherment, dataEncipherment	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA al servei de l'ADMINISTRACIÓ en programari	critical, digitalSignature, keyEncipherment, nonRepudiation	clientAuth, emailProtection	critical,CA:false
SEGELL D'EMPRESA (Persona Jurídica) en HSM - Segell Electrònic	critical, nonRepudiation	clientAuth, emailProtection	critical,CA:false

SEGELL D'EMPRESA (Persona Jurídica) en HSM – IDENTITAT	critical, digitalSignature	clientAuth, emailProtection	critical,CA:false
SEGELL D'EMPRESA (Persona Jurídica) en programari	critical, digitalSignature, keyEncipherment, dataEncipherment, nonRepudiation	clientAuth, emailProtection	critical,CA:false
REPRESENTANT PERSONA JURÍDICA en HSM - Segell Electrònic	critical, nonRepudiation	clientAuth, emailProtection	critical,CA:false
REPRESENTANT PERSONA JURÍDICA en HSM – IDENTITAT	critical, digitalSignature	clientAuth, emailProtection	critical,CA:false
REPRESENTANT PERSONA JURÍDICA en programari	critical, digitalSignature, keyEncipherment, nonRepudiation	clientAuth, emailProtection	critical,CA:false
Certificat d'actuació d'Administració, Òrgan o Entitat de Dret Públic en HSM	critical, digitalSignature, keyEncipherment, dataEncipherment, nonRepudiation	clientAuth, emailProtection	critical,CA:false
Certificat d'actuació d'Administració, Òrgan o Entitat de Dret Públic en programari	critical, digitalSignature, keyEncipherment, dataEncipherment, nonRepudiation	clientAuth, emailProtection	critical,CA:false

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

4.5.2 Relying party public key and certificate usage

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

4.6. Certificate renewal

4.6.1 Circumstance for certificate renewal

Regarding the technical certificates, ie secure server, business seal and code signing, renewal is not allowed, and the process corresponding to a new issue must be carried out.

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

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

ROOT certificates are issued in a new procedure through a process created for this purpose.

OCSP certificates are issued periodically and no renewal processes are established.

4.6.2 Who may request renewal

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

4.6.3 Processing certificate renewal requests

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

In the case of renewal of natural person final entity certificates, the issuance of a certificate without physical presence is allowed up to a period of 5 years from the last physical registration. Once the period marked has expired, the Signatory must carry out a process of issuance in person equal to that carried out for the first issuance. Under these practices, if at the time of renewal of the certificate no more than 5 years have elapsed, the physical presence of the holder will not be required.

Under these practices, if any information of the Signatory or the key holder has changed, a new registration and issuance must be made, as set forth in the corresponding sections of this document.

Camerfirma performs certificate renewals by always issuing new keys, therefore, the technical issuing process is the same as the one followed when a new request is made.

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

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

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

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

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

4.6.4 Notification of new certificate issuance to subscriber

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

4.6.5 Conduct constituting acceptance of a renewal certificate

As stipulated in section 4.4.1 of this document.

4.6.6 Publication of the renewal certificate by the CA

As stipulated in section 4.4.2 of this document.

4.6.7 Notification of certificate issuance by the CA to other entities

In some cases, end-entity certificates are sent to national supervisors who regulate the activities of certification authorities.

The OCSP certificates are communicated to different government bodies that have a platform for certificate validation.

ROOT and SubCA certificates are notified to the national supervisor for incorporation into the TSL. In addition to an information repository managed by Mozilla, which incorporates information on certification authorities - CCADB. This database is used by various commercial programs to manage their trusted warehouses

4.7. Certificate re-key

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

4.7.1 Circumstance for certificate re-key

Certificate rekey will ordinarily take place as part of a Certificate renewal.

4.7.2 Who may request certification of a new public key

As stated in section 4.6.2

4.7.3 Processing certificate re-keying requests

As stated in section 4.6.3

4.7.4 Notification of new certificate issuance to subscriber

As stated in section 4.6.4

4.7.5 Conduct constituting acceptance of a re-keyed certificate

As stated in section 4.6.5

4.7.6 Publication of the re-keyed certificate by the CA

As stated in section 4.6.6

4.7.7 Notification of certificate issuance by the CA to other entities

As stated in section 4.6.7

4.8. Certificate modification

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

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

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

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

4.8.1 Circumstance for certificate modification

Not applicable

4.8.2 Who may request certificate modification

Not applicable

4.8.3 Processing certificate modification requests

Not applicable

4.8.4 Notification of new certificate issuance to subscriber

Not applicable

4.8.5 Conduct constituting acceptance of modified certificate

Not applicable

4.8.6 Publication of the modified certificate by the CA

Not applicable

4.8.7 Notification of certificate issuance by the CA to other entities

Not applicable

4.9. Certificate revocation and suspension

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

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

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

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

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

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

However, Camerfirma will keep the information about the status of an expired certificate in its databases and accessible through the OCSP service.

Under no circumstances is the use of a revoked certificate allowed under these practices.

OCSP's response to a revoked certificate when it expires maintains the revocation status and its cause.

Due to the different nature of the OCSP and CRL services, in the event that different responses are obtained for an expired certificate, the response provided by OCSP will remain valid.

For Camerfirma the service of consulting the status of a primary certificate is the one offered by OCSP.

4.9.1 Circumstances for revocation

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

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

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

Due to circumstances affecting key or certificate security.

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

Due to circumstances affecting the security of the cryptographic device

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

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

- The relationship is terminated between the Certification Authority and the Signatory or person/entity responsible for the certificate.
- There are changes to or termination of the underlying legal relationship or cause for issuing the certificate to the Signatory or person/entity responsible for the certificate.
- The applicant breaches part of the requirements established for requesting the certificate.

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

Other circumstances

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

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

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

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

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

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

4.9.2 Who can request revocation

Certificate revocation can be requested by:

- The Subject/Signatory

- The responsible Applicant

- The Entity (via a representative)

- The RA or CA.

- Anyone established in the specific certification policies.

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

4.9.3 Procedure for revocation request

All requests must be made:

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

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

- By physically going to the RA’s offices during opening hours, showing the Subject/Signatory or Applicant’s National Identity Card.

- By sending Camerfirma a document signed by a representative with sufficient representation powers for the entity requesting certificate revocation. This form must be used to revoke Subordinate CA.

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

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

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

4.9.4 Revocation request grace period

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

4.9.5 Time within which CA must process the revocation request

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

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

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

4.9.6 Revocation checking requirement for relying parties

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

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

The CRL contains a field (NextUpdate) with the date of your next update.

4.9.7 CRL issuance frequency

AC	Frecuencia de emisión días	Duración días
Chambers of Commerce Root	**Máximo 365**	**365**
AC Camerfirma Certificados Camerales	Inmediato Máximo 1	2
AC CAMERFIRMA AAPP	Inmediato Máximo 1	2

Global Chambersign Root	**Máximo 365**	**365**
AC Camerfirma	**Máximo 365**	**365**
RACER	24 horas	48 horas
Entidad de Certificación de la Administración Pública Andorrana	24 horas	48 horas

4.9.8 Maximum latency for CRLs

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

4.9.9 On-line revocation/status checking availability

CA provides an online service to check revocations at http://www.camerfirma.com/area-de-usuario/consulta-de-certificados/

Also via OCSP queries:

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

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

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

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

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

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

The latency of publication in the OCSP service of a revocation is 1 hour

4.9.10 On-line revocation checking requirements

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

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

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

4.9.11 Other methods of disclosing revocation information

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

4.9.12 Special requirements re key compromise

Not stipulated

4.9.13 Circumstances for suspension

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

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

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

The suspension process does not apply to certificates

- From TSU.
- From CA.
- From RA Operator.

4.9.14 Who can request suspension

See section 4.9.2.

4.9.15 Procedure for suspension request

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

4.9.16 Limits on suspension period

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

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

4.10. Certificate status services

4.10.1 Operational characteristics

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

4.10.2 Service availability

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

4.10.3 Optional features

Not stipulated.

4.11. End of subscription

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

4.12. Key Escrow and recovery

4.12.1 Key escrow and recovery policy and practices

For certificates in hardware support, it is the user who generates and stores the private key on the cryptographic card delivered by the provider.

For certificates issued in software, Camerfirma stores the user keys in PKCS#12 format in order to resend them in case of problems with downloading and installation. This information is stored only for 3 calendar days. After this period these keys are deleted from the system. These keys are not included in the system backup services.

For certificates issued in Centralized Device (CKC) Camerfirma stores the keys generated for the user in a secure HSM device certified at least FIPS-140-2 level 3 or EAL 4+, providing the corresponding mechanisms to guarantee the unique control of the key.

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

4.12.2 Session key encapsulation and recovery policy and practices

Not stipulated.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1. Physical controls

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

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

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

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

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

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

5.1.1 Site location and construction

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

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

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

5.1.2 Physical access

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

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

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

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

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

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

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

5.1.3 Power and air conditioning

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

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

5.1.4 Water exposures

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

5.1.5 Fire prevention and protection

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

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

5.1.6 Media storage

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

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

5.1.7 Waste disposal

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

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

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

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

5.1.8 Off-site 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 Trusted roles

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

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

- Duties associated with the function.
- Level of access.
- Monitoring of the function.
- Training and awareness.
- Required skills.

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

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

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

System administrator tasks are incompatible with certification tasks and they cannot carry out operations auditor tasks.

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

The tasks of the CA administrator are incompatible with the tasks of certification and systems.

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

The tasks of the AC operator are incompatible with those of the AC administrator and he cannot perform the tasks of an auditor or internal auditor.

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

AR operator operations are incompatible with AR administrator operations and cannot perform internal or external audit tasks.

Revocation operator:
The tasks of the revocation operator are incompatible with the tasks of Audit

Security Manager:
Responsible for coordinating, controlling and complying with the security measures defined by the Camerfirma security policies. The security manager is be responsible for aspects related to information security: logical, physical, networks, organizational, etc.

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

5.2.2 Number of persons required per task

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

5.2.3 Identification and authentication for each role

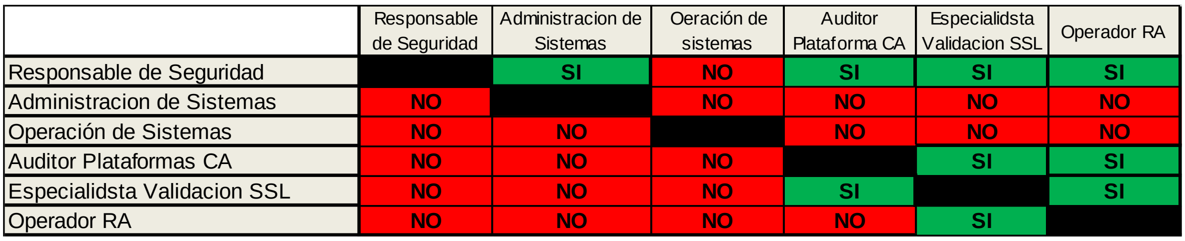
The internal auditor assigns the people for each role; this auditor must ensure that each person carries out the procedures to which he/she is assigned.

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

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

5.2.4 Roles requiring separation of duties

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



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

5.2.5 Switching the PKI management system on and off.

The PKI system is formed by the following modules:

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

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

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

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

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

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

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

The module switch-off sequence is:

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

The switching on process is carried out in reverse.
Internal reference document: IN-2005-05-01-Manual switching off procedure.

5.3. Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

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

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

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

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

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

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

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

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

Reference documentation:

- IN-2005-02-07-Personnel duties and responsibilities.
- IN-2005-02-17-Human Resource Management
- IN-2008-00-06-Job Profile Format
- IN-2008-00-09-Training Logs
- IN-2006-02-03-Security Organization

5.3.2 Background check procedures

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

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

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

5.3.3 Training requirements

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

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

Training includes the following content:

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

5.3.4 Retraining frequency and requirements

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

5.3.5 Job rotation frequency and sequence

Not stipulated

5.3.6 Sanctions for unauthorized 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 Independent contractor requirements

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

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

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

Reference documentation:

- IN-2006-05-02-Clauses that apply to external developers
- IN-2005-02-17-Human Resources Management

5.3.8 Documentation supplied to personnel

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

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

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

Reference documentation: IN-2005-02-17-Human Resources Management

5.4. Audit logging procedures

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

5.4.1 Types of events recorded

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

The following events are recorded:

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

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

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

Camerfirma maintains a system that guarantees:

- Enough space for logs storage

- That the log files are not rewritten.
- That the information stored includes at least: type of event, date and time, user that executes the event and result of the operation.
- The log files will be stored in structured files that can be incorporated into a database for further exploration.

5.4.2 Frequency of processing log

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

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

5.4.3 Retention period for audit logs

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

5.4.4 Protection of audit log

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

They are stored in fireproof devices.

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

Audit log files can only be accessed by authorised persons.

Devices are always handled by authorised personnel.

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

5.4.5 Audit Log backup procedures

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

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

A copy is also kept at an external custody centre.

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

5.4.6 Audit collection system (internal vs. external)

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

5.4.7 Notification to event-causing subject

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

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

5.4.8 Vulnerability assessments

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

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

Every month Camerfirma performs a system analysis to detect suspicious activity. This report is executed by an external company incorporated:

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

Camerfirma corrects any reported problem and is recorded by the systems department.

5.5. Records Archival

5.5.1 Types of records archived

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

- Any system audit data. PKI, TSA and OCSP
- Any data related to certificates, including contracts with Signatories and the RA. The data relating to their identification and location.

- Requests to issue and revoke certificates.
- Type of document submitted in the license application.
- Identity of the Registration Authority that accepts the certificate application.
- Unique identification number provided by the previous document.
- Any issued or published certificates.
- Issued CRLs or logs of the status of created certificates.
- Log of created keys.
- Communications between PKI elements.
- Certification Policies and Practices

Camerfirma is responsible for correctly filing all this material.

5.5.2 Retention period for archive

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

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

5.5.3 Retention period for archive

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

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

5.5.4 Archive backup procedures

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

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

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

5.5.5 Requirements for time-stamping of records

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

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

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

5.5.6 Archive collection system (internal or external)

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

5.5.7 Procedures to obtain and verify archive information

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

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

5.6. Key Changeover

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

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

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

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

5.7. Compromise and disaster recovery

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

The commitment of the algorithms or associated parameters used in the generation of digital certificates or associated services are also incorporated into the contingency and business continuity plan.

5.7.1 Incident and compromise handling procedures

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

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

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

If any equipment is damaged or rendered inoperative but the Private Keys are not destroyed, the operation should be re-established as quickly as possible, giving priority to the ability to generate Certificate status information according to Camerfirma's disaster recovery plan.

5.7.3 Entity private key compromise procedures

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

If the security of a root key is compromised:

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

5.7.4 Business continuity capabilities after a disaster

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

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

5.8. CA or RA termination

Before Camerfirma ceases its activity, it will:

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

All these activities will be included in detail in the internal document CONF-2003-00-01 Plan of Continuity and Availability and Cessation of Activity of AC Camerfirma SA.

6. Technical Security Controls

6.1. Key pair generation and installation

6.1.1 Key pair generation

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

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

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

CA	Longitud de claves	Algoritmo de firma	Año creación	Caducidad
Chambers of Commerce Root	2.048 bits	Sha1WithRSAEncryption	2.003	30/09/2037
AC Camerfirma Express Corporate Server	2.048 bits	Sha1WithRSAEncryption	2.007	09/02/2034
AC Camerfirma Certificados Camerales	2.049 bits	Sha1WithRSAEncryption	2.004	09/02/2034
AC CAMERFIRMA AAPP	2.048 bits	Sha1WithRSAEncryption	2.010	20/02/2022
Global Chambersign Root	2.048 bits	Sha1WithRSAEncryption	2.003	30/09/2037
AC Camerfirma	2.048 bits	Sha1WithRSAEncryption	2.003	14/11/2033
RACER	2.048 bits	Sha1WithRSAEncryption	2.003	04/12/2023

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

Reference documentation:

- CONF-00-2012-01 RECORDS from key creation events.
- CONF-00-2012-02/04 Key generation SCRIPTS.
- CONF-00-2012-05 Auditor Report.
- CONF-00-2012-03 Distributing keys among operators.

6.1.1.1 Creating the Signatory’s key pair

The Subject/Signer keys can be created in the Subject by means of hardware devices (QSCD) or software authorized by Camerfirma or can be created by Camerfirma in software format PKCS#12.

In SSL/TLS certificates the client generates the key pair under the control of the corresponding page management system.

If the certificate is qualified and requires a qualified signature creation device, this certificate will only be used with such devices to perform electronic signatures.

The STATUS management platform generates with its own resources a robust random password and a private key protected with this password using the 3DES algorithm. From that private key it generates a certificate signing request in PKCS#10 format. With that request the CA performs the signature of the Signer's certificate. The certificate is delivered to the user in a PKCS#12 file in which the certificate itself and the private key associated with it are included. The password for the private key and the PKCS#12 file is never clear in the system.

The keys are generated using the RSA public key algorithm.

The keys can also be created on a remote system using the Web services layer to generate a PKCS#10 request and the corresponding PKCS#7 collection.

In a CKC centralised key management system, the keys are generated on an HSM certified as a qualified signature creation device in the list published by the European Commission Member States: https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds .

The keys have a minimum length of 2048 bits.

6.1.1.2 Key creation hardware/software

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

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

6.1.2 Private key delivery to subscriber

See section 3.2.1

6.1.3 Public key delivery to certificate issuer

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

6.1.4 CA public key delivery to relying parties

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

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

6.1.5 Key Sizes

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

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

6.1.6 Public key parameters generation and quality checking

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

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

6.1.7 Key Usage Purposes (as per X.509 v3 key usage field)

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

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

6.2.1.1 The CA's private key

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

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

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

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

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

- CONF-2016-04-02-Proteccion y activación de claves de CA Online

- CONF-2012-04-10 - Script Ceremonia de emisión de certificados.

6.2.1.2 The Signatory's private key

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

When stored in software format Camerfirma will provide the appropriate configuration instructions for safe use.

In a CKC central key management system, the keys are generated in an HSM certified as a qualified signature creation device in the list published by the European Commission member states: https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds.

Regarding the cryptographic devices distributed by Camerfirma to host qualified certificates, they all meet the requirements of qualified signature creation devices and are therefore suitable for qualified signature generation.

The information regarding the process of creation and custody of keys used by Camerfirma is incorporated into the digital certificate itself, through the corresponding OID allowing the User Party to act accordingly.

6.2.2 Private key (n out of m) multi-person control

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

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

6.2.3 Private key escrow

Camerfirma does not store or copy the private keys of the owners.

Exceptions:

- In case of certificates for information encryption, Camefirma keeps a copy of the key.
- In a CKC central key management system, the keys are generated in an HSM certified as a qualified signature creation device in the list published by the European Commission member states: https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds.

6.2.4 Private key backup

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

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

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

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

In a CKC centralised key management system, the signatory's keys can be backed up under the terms of the relevant regulations.

Camerfirma keeps records on CA private key management processes.

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

6.2.5 Private key archival

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

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

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

AC Camerfirma puts at the disposal of the certificate holders whose private key is generated by the provider from the moment of the delivery of this certificate the download of the file PKCS#12, which contains this private key and its associated certificate, during three working days.

Camerfirma keeps records on CA private key management processes.

6.2.6 Private key transfer into or from a cryptographic module

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

Intermediate CA keys are stored in online network HSM equipment, so that they can be accessed from the PKI applications for certificate generation.
In a CKC signatory central key management system as described in the device manufacturer's manual.

6.2.7 Private key storage on cryptographic module

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

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

6.2.8 Method of activating private key

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

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

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

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

Camerfirma keeps records on CA private key management processes.

Notes on the centralized key management system:
In the case of implementation of a centralized signature system the subscriber has a unique and secret activation password that will enable the remote private key to be activated in the same way as it would in a local keystore. Before activating the key, the user must have authenticated the centralized management application where the user's identity is associated with the key stored in the centralized device.

6.2.9 Method of deactivating private key

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

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

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

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

6.2.10 Method of destroying private key

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

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

Backups are destroyed securely.

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

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

Camerfirma keeps records on CA private key management processes.

Reference documentation: IN-2006-05-01-Destrucción Claves de Usuario

6.2.11 Cryptographic Module Rating

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

In a CKC centralised key management system, the keys are generated in an HSM certified as a qualified signature creation device in the list published by the European Commission member states: https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds.

6.3. Other aspects of key pair management

6.3.1 Public key archival

The CA, in compliance with the provisions of article 20 f) of the LFE 59/2003, shall keep its files for a minimum period of fifteen (15) years, as long as the technology allows it. The documentation to be kept includes the public key certificates issued to its subscribers and its own public key certificates.

6.3.2 Certificate operational periods and key pair usage periods

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

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

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

6.4. Activation data

6.4.1 Activation data generation and installation

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

In software. The certificate is generated by the provider and is delivered in a standardized PKCS#12 file protected by a password generated by the management application and delivered to the subject by means of the mail associated with the digital certificate.

In hardware device. The cards used by Camerfirma are generated at the registration desk protected with a PIN and PUK calculated at the factory. This information is sent by the management platform to the subject by means of the mail associated with the digital certificate. The subject has a software to change the PIN and PUK of his card.

In Hardware Device (HSM) of third party. AC Camerfirma homologates third party devices, although these have an independent management. The keys are generated in an independent ceremony and a certificate issue request is given to Camerfirma together with the ceremony minutes.

In the centralized management platform, the keys are generated in an HSM cryptographic device protected by a master key of the device and by the activation data of the generated key known only to the associated certificate holder. The platform allows a double activation control to be activated via OTP.

6.4.2 Activation data protection

The activation data are communicated to the subject through a separate channel to the PKI management platform. AC Camerfirma does not store this information in its database when we talk about certificates in software or hardware format. In the centralized platform we do not store them being known and guarded by the holder. The data can be sent back to the subject on request prior to the mail associated with the certificate, and will be effective as long as the user has not made a change in them previously.

In a CKC signatory centralised key management system as described in the device manufacturer's manual.

6.4.3 Other aspects of activation data

Not stipulated.

6.5. Computer security controls

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

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

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

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

6.5.1 Specific computer security technical requirements

Each Camerfirma server includes the following functions:

- access control to CA services and privilege management.
- separation of tasks for managing privileges
- identification and authentication of roles related to identities
- the Signatory's and CA's log file and audit data
- audit of security events
- self-diagnosis of security related to CA services
- Key and CA system retrieval mechanisms

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

6.5.2 Computer security rating

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

6.6. Life cycle technical controls

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

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

As regards hardware devices

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

For devices used in the Central Key Management platform: The device that stores the keys is FIPS-104-2 level 3 or EAL4+ certified and authorized by the national supervisor for services listed as QSCDManagedOnBehalf.

6.6.1 System development controls

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

In response to the intrusion and vulnerability analyses, the adaptations of the systems and applications that may have security problems are made and to the security alerts received from the managed security services contracted with third parties, the corresponding RFCs (Request for Changes) are executed for the incorporation of the security patches or the update of the versions with problems.

The RFC incorporates and documents the measures taken for the acceptance, execution or denial of such change.

In cases where the execution of the update or correction of an issue incorporates a vulnerability or significant risk, it is incorporated into the risk analysis and alternative controls are executed until the level of risk is acceptable.

Reference documentation:

- IN-2006-05-02-Clauses that apply to external developers
- IN-2006-03-04-Systems and Software Change Control

6.6.2 Security management controls

6.6.2.1 Security management

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

An annual training plan has been established for such purposes.

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

6.6.2.2 Data and asset classification and management

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

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

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

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

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

6.6.2.3 Management procedures

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

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

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

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

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

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

Reference documentation:

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

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

Related documentation:

- IN-2010-10-10 Configuration management
- IN-2010-10-05 Capacity Management
- IN-2010-10-03 Availability Management

- IN-2010-10-01 Service Level Management
- IN-2010-10-00 IT Services Management Manual
- IN-2010-10-13 New Services Planning

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

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

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

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

6.6.2.4 Access system management

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

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

In particular:

General CA

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

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

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

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

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

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

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

Revocation management

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

Revocation status

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

6.6.2.5 Managing the cryptographic hardware lifecycle

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

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

Camerfirma records all the pertinent information of the device to add to the asset catalogue.

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

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

The cryptographic hardware device is only handled by trustworthy personnel.

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

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

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

6.6.3 Life cycle security controls

Not stipulated

6.7. Network security controls

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

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

The policy used for the configuration of the systems and security elements is to start from an initial state of total blocking and to open the services and ports necessary for the execution of the services. As part of the tasks to be carried out in the systems department, the revision of the accesses is incorporated.

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

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

6.8. Time-stamping

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

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

7. Certificate, CRL, and OCSP profiles

7.1. *Certificate Profile*

Certificate profiles comply with RFC 5280.

All qualified or recognised certificates issued in accordance with this policy comply with standard X.509 version 3, and RFC 3739 and the different profiles described in the EN 319 412 standard.

The profile records for these certificates can be requested from gestion_soporte@camerfirma.com or by telephone 902 361 207

7.1.1 Version number(s)

Camerfirma issues X.509 certificates Version 3

7.1.2 Certificate extensions

Certificate extension documents are described in the profile files. The profile records can be requested from gestion_soporte@camerfirma.com or by telephone 902 361 207

7.1.3 Algorithm object identifiers

The signature algorithm object identifier is

- 1.2.840.113549.1.1.5 - sha1withRSAEncryption
- 1.2.840.113549.1.1.11 - sha256WithRSAEncryption

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

7.1.4 Name forms.

Certificates must contain the information that is required for its use, as determined by the corresponding authentication policy, digital signature, encryption or digital evidence.

In general, certificates for use in the public sector must contain the identity of the person who receives them, preferably in the Subject Name or Subject Alternative Name fields, including the following data:

- The full name of the Signatory person, certificate holder or represented, in separate fields, or indicating the algorithm that allows the separation automatically.
- Name of the legal entity, where applicable.
- Numbers of the corresponding identification documents, in accordance with the law applicable to the Signatory person, certificate holder or represented, whether a natural person or a legal entity.

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

The exact semantics of the names are described in the profile sheets. The profile sheets can be requested at https://www.camerfirma.com/ayuda/soporte/ or by phone at 902 361 207

7.1.5 Name constraints

Camerfirma may use name restrictions (using the “name constraints” certificate extension) in Subordinate CA certificates issued to third parties so that only the set of certificates allowed in this extension can be issued by the Subordinate CA.

7.1.6 Certification Policy object identifier

All Camerfirma’s certificates has a policy identifier that starts from the base 1.3.6.1.4.1.17326.

Govern d’Andorra = 2.16.20.2.1.3.1

7.1.7 Usage of Policy Constraints extension

Camerfirma may use policy restrictions (using the “*policy constraints*” certificate extension) in Subordinate CA certificates issued to third parties so that only the set of certificates allowed in this extension can be issued by the Subordinate CA.

7.1.8 Policy qualifiers syntax and semantics

Not stipulated

7.1.9 Processing semantics for the critical Certificate Policies extension

The “Certificate Policy” extension identifies the policy that defines the practices that Camerfirma explicitly associates with the certificate. The extension may contain a qualifier from the policy. See 7.1.6.

7.2. CRL Profile

The CRL profile matches the one proposed in the relevant certification policies. The CRLs are signed by the CA that issued the certificates.

The CRL's detailed profile can be requested from gestion_soporte@camerfirma.com or by telephone 902 361 207.

7.2.1 Version number(s)

The CRLs issued by Camerfirma are version 2.

7.2.2 CRL and CRL entry extensions

Those established in the certification policies. The detailed profile of the CRL and its extensions can be requested from gestion_soporte@camerfirma.com or by telephone 902 361 207.

7.3. OCSP Profile

7.3.1 Version number (s)

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

7.3.2 OCSP Extensions

The profile of the OCSP responder certificates can be obtained from gestion_soporte@camerfirma.com or by telephone 902 361 207.

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

8. Compliance Audit and Other Assessment

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

Camerfirma's objectives in relation to security and quality have essentially involved obtaining ISO/IEC 27001, ISO/IEC 20000 certification and carrying out biennial audits on its certification system, and essentially on the Registration Authorities, in order to guarantee compliance with internal procedures.

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

In order to comply with eIDAS requirements, AC Camerfirma undertakes a biennial compliance evaluation as established in the regulation of the following standards: EN 319 401, EN 319 411-1, EN 319 411-2, EN 319 421.

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

AC Camerfirma is subject to a biennial Spanish Personal Data Protection Act audit.

AC Camerfirma performs an internal audit on entities that have obtained a Subordinate CA or TSU certificate and that issue and manage certificates with their own technical and operational resources. In this audit, Camerfirma randomly checks a number of certificates issued by this registration authority, ensuring that the evidence collected is correct and sufficient for the issuance of the certificate.

8.1. *Frequency or circumstances of assessment*

Camerfirma conducts an annual compliance audit, in addition to the internal audits performed on a discretionary basis.

- ISO 27001 and ISO20000 auditing on a three-year cycle with annual reviews.
- WEBTRUST for CA, WEBTRUST SSL BR, WEBTRUST EV SSL annually.
- eIDAS Conformity Assessment, biennial with annual review
- Spanish Personal Data Protection Act audit, biennial with annual review.
- RA audits on a discretionary basis.
- Internal Audits, External Subordinate CAs, External TSUs, on a discretionary basis.
- Vulnerability audit quarterly.
- Penetration test yearly.

8.1.1 External Subordinate CA audits.

Through its auditors, AC Camerfirma conducts an annual audit on the organizations that have obtained a Subordinate CA or TSA certificate and that issue certificates with their own technical and operational resources. This audit can be replaced by a favourable *WebTrust for CA* and/or *WebTrust for EV* audit certificate as applicable to the certificates issued.

8.1.2 Auditing the Registration Authorities

Every RA is audited. These audits are performed at least every two years on a discretionary basis and based on a risk analysis. The audits check compliance with the Certification Policy requirements in relation to undertaking the registration duties established in the signed service agreement.

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

Reference documentation regarding the RA audit process are:

- IN-2010-04-12-RA Security Evaluation Procedure
- IN-2010-04-15-Ficha de la visita de evaluación.doc
- IN-2010-04-16-Check List
- IN-2006-03-08-RA Work Procedures.
- IN-2010-04-17-Evaluation Report

8.1.3 Internal Audits

In addition to the previously defined audits, AC Camerfirma performs internal quality controls on 3% of the server certificates issued. The audit period starts immediately after the last sample was taken.

The audit consists of the revision of the veracity and documentary support of the data incorporated in the certificate selected in the sample.

The department in charge will make a report on the audit performed.

8.2. Identity/qualifications of assessor

Audits are performed by the following widely recognized external independent companies in computer security, Information Systems security and Certification Authority compliance audits:

- For WEBTRUST - AUREN audit http://www.auren.com.
- For ISO27001/20000 ISO 9001 -AENOR audits. http://www.aenor.es
- For internal audits / RA / AC subordinate, TSA LOPD/RGPD - AUREN http://www.auren.com/

8.3. Assessor's relationship to assessed entity

The auditing companies are independent and of recognized prestige, having specialized departments in the realization of computer audits in the management of digital certificates and trust services, so there is no conflict of interest that could distort their performance in relation to the CA.

There is no link or financial or organic dependence between the audit companies and AC Camerfirma.

8.4. Topics covered by assessment

In general terms, the audits verify:

a) That Camerfirma has a system that guarantees service quality.
b) 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.
c) That Camerfirma properly manages the security of its information systems.
d) In the OV and EV certificates, the audit checks variance with the policies established by CABFORUM in the "*Baseline Requirements*" as well as "*EV SSL Certificate guidelines*".

In general, the elements audited are:

- Camerfirma processes, RAs and related elements in the issuing of TSA timestamp certificates and validation of services in OCSP line.
- Information systems.
- Protecting the data processing centre.
- Documentation required for each type of certificate.
- Verification that the RA operators know AC Camerfirma's CPS and Policies

8.5. Actions taken as a result of deficiency

Once the compliance report from the audit is received, Camerfirma discusses any deficiencies found with the entity that carried out the audit and develops and implements a corrective plan in order to address the shortcomings.

If the audited entity is unable to develop and/or implement the plan within the time frame requested, or if the deficiencies pose an immediate threat to the system's security or integrity, the policy authority must be notified immediately, and may take the following actions:

- Cease operations temporarily.
- Revoke the corresponding certificate and restore infrastructure.
- Terminate service to the Entity.
- Other complementary actions as may be needed.

8.6. Communication of results

The communication of results will be carried out by the auditors who have carried out the evaluation to the person in charge of security and regulatory compliance. It is carried out in an act with the presence of the corporate management. The audit certificate is published on the Camerfirma website.

9. Other business and legal matters

9.1. Fees

9.1.1 Certificate issuance or renewal fees

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

http://www.camerfirma.com/certificados/ or by prior consultation with the Camerfirma support department athttps://secure.camerfirma.com/incidencias/ or by telephone 902 361 207.

The specific price is published for each type of certificate, except those subject to previous negotiation.

9.1.2 Certificate access fees

Access to certificates is free-of-charge, although AC Camerfirma applies controls in order to avoid mass certificate downloads. Any other situation that Camerfirma deems must be considered in this respect will be published on Camerfirma’s website http://www.camerfirma.com/certificados/ or by prior consultation with the Camerfirma support department at https://secure.camerfirma.com/incidencias/ or by telephone: 902 361 207.

9.1.3 Revocation or status information access fees

Camerfirma provides free access to information relating to the status of certificates or revoked certificates via certificate revocation lists or via its website http://www.camerfirma.com/area-de-usuario/consulta-de-certificados/.

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

9.1.4 Fees for other services

Access to the content of this CPS is free-of-charge on Camerfirma's website https://policy.camerfirma.com.

9.1.5 Refund policy.

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

The correct issuance of the digital certificate, be it in the support that is, supposes the beginning of the execution of the contract, with what, according to the General Law for the Defense of Consumers and Users (RDL 1/2007) in such cases , the Subject / Holder loses his right of withdrawal.

9.2. Financial Responsibility

9.2.1 Insurance coverage

Camerfirma, in its role as a CSP, has a public liability insurance policy that covers its liabilities to pay compensation for damages and losses caused to the users of its services: the Subject/Signatory and the User Party and third parties, for a total amount of 3,700,000 euros.

9.2.2 Other assets

Not stipulated

9.2.3 Insurance or warranty coverage for end-entities

See section 9.2.1

9.3. Confidentiality of business information

9.3.1 Scope of business information

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

Camerfirma has established a policy for processing confidentiality agreement information and forms, which anyone accessing confidential information must sign.

Reference documentation:

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

9.3.2 Information not within the scope of confidential information

Camerfirma considers the following information not confidential:

a) The contents of this CPS and the Certification Policies
b) The information contained in the certificates.
c) Any information whose accessibility is prohibited by current law.

9.3.3 Responsibility to protect confidential information

Camerfirma is responsible of the protection of the confidential information generated or communicated during all operations. Delegated parties, as the entities managing subordinate Issuing CAs or Registration Authorities, are responsible for protecting confidential information that has been generated or stored by their own means.

For end entities, the certificate subscribers are responsible to protect their own private key and all activation information (i.e. passwords or PIN) needed to access or use the private key.

9.3.3.1 Disclosure of information about certificate revocation/suspension

Camerfirma discloses information on the suspension or revocation of a certificate by periodically publishing corresponding CRLs.

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

Camerfirma has an online query service for the status of certificates based on the OCSP standard at http://ocsp.camerfirma.com. The OCSP service provides standardized responses about the status of a digital certificate under the RFC 2560; in other words, whether the certificate consulted is active, revoked or whether it has been issued by the certification authority.

The policy for dissemination of information about certificate revocation in External Subordinate CAs with use of proprietary technology is based on their own CPS.

9.3.3.2 Sending information to the Competent Authority

Camerfirma will provide the information that the competent authority or corresponding regulatory entity requests in compliance with current law.

9.4. Privacy of Personal Information

9.4.1 Privacy plan

In any case, Camerfirma complies with current regulations regarding data protection, in particular, it has adapted its procedures to the REGULATION (EU) 2016/679 General of Data Protection (RGPD). In this sense, this document serves, in accordance with Law 59/2003, of Electronic Signature (article 19.3) and the eIDAS Regulation (article 24.2.f) as a security document.

Reference documentation: IN-2006-05-11-Compliance with legal requirements

9.4.2 Information treated as private

Personal information about an individual that is not publicly available in the contents of a certificate or CRL is considered private.

9.4.3 Information not deemed private

The personal information about an individual available in the contents of a certificate or CRL, is considered as non-private when it is necessary to provide the contracted service, without prejudice to the rights corresponding to the holder of the personal data under the LOPD/RGPD legislation.

9.4.4 Responsibility to protect private information

It is the responsibility of the controller to adequately protect private information.

9.4.5 Notice and consent to use private information

Before entering into a contractual relationship, Camerfirma will offer interested parties prior information about the processing of their personal data and the exercise of rights, and, if applicable, will obtain the mandatory consent for the differentiated treatment of the main treatment for the provision of contracted services.

9.4.6 Disclosure pursuant to judicial or administrative process

Personal data that are considered private or not, may only be disclosed if necessary for the formulation, exercise or defense of claims, either by a judicial procedure or an administrative or extrajudicial procedure.

9.4.7 Other information disclosure circumstances

Personal data will not be transferred to third parties except legal obligation.

9.5. Intellectual Property Rights

Camerfirma owns the intellectual property rights on this CPS. The CPS of Subordinate CAs associated with Camerfirma hierarchies is owned by Camerfirma, without prejudice to the assignments of use of their rights in favour of Subordinate CAs and without prejudice to the contributions of the Subordinate CAs that are owned by them.

9.6. Representations and Warranties

9.6.1 CA representations and warranties

9.6.1.1 CA

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

- Adhere to the provisions within the scope of this CPS and the corresponding Certification Policies.
- Protect its private keys and keep them secure.
- Issue certificates in accordance with this CPS, the Certification Policies and the applicable technical standards.
- Issue certificates in accordance with the information in its possession and which do not contain errors.
- Issue certificates with the minimum content defined by current law for qualified or recognised certificates.
- Publish issued certificates in a directory, respecting all legal provisions regarding data protection.
- Suspend and revoke certificates in accordance with this Policy and publish the revocations in the CRL.
- Inform Subjects/Signatories about the revocation or suspension of their certificates, on time and in accordance with current law.
- Publish this CPS and the Certification Policies on its website.
- Report changes to this CPS and the Certification Policies to the Subjects/Signatories and its associated RAs.
- Do not store or copy the Subject/Signatory’s signature creation data except for encryption certificates and when it is legally provided for or allowed to be stored or copied.
- Protect data used to create the signature while in its safekeeping, if applicable.
- Establish data creation and custody systems in the aforementioned activities, protecting data from being lost, destroyed or forged.
- Keep data relating to the issued certificate for the minimum period required by current law.
- For certificates issued in a centralized device (CKC), to guard with due diligence the private keys of the certificates to which only the Subjects/Holders can have access.

Camerfirma’s responsibility

Article 22.1 of the Law on Digital Signatures establishes that:
Certification service providers are responsible for damages and losses caused to any person during their activities in the event they breach the obligations established in this Law.

The certification service provider regulated herein shall be held liable in accordance with general regulations on contractual or non-contractual liability, as applicable, although the certification service provider must prove that it acted with due professional diligence.

Camerfirma is responsible for any damages or losses caused to users of its services, whether the Subject/Signatory or the User Party, and other third parties in accordance with the terms and conditions established under current law and in the Certification Policies.

In this sense, Camerfirma is the only party responsible for (i) issuing the certificates, (ii) managing them throughout their lifecycle and (iii) in particular, if necessary, in the event of suspension and revocation of the certificates. Specifically, Camerfirma is fundamentally responsible for:

- The accuracy of the information contained in the certificate on the date of issue by confirming the applicant's details and the RA practices.
- Guaranteeing that when the certificate is delivered, the Subject/Signatory is in possession of the private key relating to the public key given or identified in the certificate when required, by using standard request forms in PKCS#10 format.
- Guaranteeing that the public and private keys work in conjunction with each other, using certified cryptographic devices and mechanisms.
- That the certificate requested and the certificate delivered match.
- Any liability established under current law.

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

9.6.1.2 External Subordinate CA.

External Subordinate CAs are CAs incorporated into the root CA's hierarchy but are owned by a different organization and may or may not use a different technique or infrastructure.

- Protect their private keys.
- Issue certificates pursuant to certification policies and/or corresponding CPS.
- Issue certificates that are free from errors.
- Publish issued certificates in a directory, respecting all legal provisions regarding data protection.
- Allow an annual audit by AC Camerfirma.
- Safeguard, for the duration established by law, the documentary information and systems that have been used or generated for issuing certificates.
- Notify AC Camerfirma of any incident in the delegated activity.

Responsibility of the Subordinate CA (Internal/External).

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

9.6.2 RA representations and warranties

RAs are entities that the CA appoints to register and approve certificates; therefore, the RAs also carry out the obligations defined in the Certification Practices for issuing certificates, particularly to:

- Adhere to the provisions of this CPS and the Certification Policy.
- Protect their private keys that are used for exercising their functions.
- Check the identity of the Subjects/Signatories and Applicants of certificates when necessary, definitively proving the Signatory's identity, for individual certificates, or the key holder, for organization certificates, pursuant to the provisions of the corresponding sections of this document.
- Check the accuracy and authenticity of information provided by the Applicant.
- Provide the Signatory, for individual certificates, or the future key holder, for organization certificates, access to the certificate.
- If applicable, deliver the corresponding cryptographic device.
- Keep the documents provided by the applicant or Signatory on file for the period required by current law.
- Respect contract provisions signed with Camerfirma and with the Subject/Signatory.
- Inform Camerfirma about the causes for revocation, when known.
- Provide basic information about the certificate's policy and use, especially including information about Camerfirma and the applicable Certification Practices Statement, as well as their obligations, powers and responsibilities.
- Provide information about the certificate and the cryptographic device.
- Compile information and evidence about the certificate holder or receiver and, if applicable, the cryptographic device, and acceptance of such elements.
- Report on the attribution method exclusive to the private key holder and, if applicable, the cryptographic device’s certificate activation data, according to this document's corresponding sections.

These obligations are even in cases of entities delegated by these such as points of physical verification.

The information about the Signatory’s use and responsibilities is provided once the terms of use are accepted prior to the confirmation of the certificate application and via email.

The RAs’ responsibility

The RAs sign a service provision agreement with Camerfirma, by virtue of which Camerfirma delegates registration duties to the RAs, which mainly consist of:

1.- Obligations prior to issuing a certificate.

a) Informing applicants about signing their obligations and responsibilities.
b) Properly identifying applicants, who must be trained or authorised to request a digital certificate.

c) Checking the validity of the applicant's details and the Entity's details, if there is a contractual relationship or powers of representation.
d) Accessing the Registration Authority application to process requests and issued certificates.

2.- Obligations once the certificate has been issued.

a) Signing Digital Certification Service Provision agreements with applicants. In most issuance processes, this contract is formalised by accepting the conditions on the websites that are part of the process of issuing the certificate. The certificate cannot be issued without the terms of use having previously been accepted.
b) Maintaining the certificates while they are still in force (expiry, suspension, revocation).
c) Filing copies of submitted documentation and the agreements signed by the applicants in accordance with the Certification Policies published by Camerfirma and current law.

Therefore, the RAs are responsible for any consequences due to non-compliance of registration duties, and undertake to adhere to Camerfirma's internal regulations (Policies and CPS), which the RAs must keep perfectly controlled and which they must use as guidelines.

In the event of a claim from a Subject, Entity or user, the CA must offer proof that it has acted diligently and if there is evidence that the cause of the claim is due to incorrect data validation or checking, the CA can hold the RA liable for the consequences, in accordance with the agreement signed with the RAs. Because, although legally the CA is the legal entity liable to the Subject, an Entity or User Party, and the Subject, an Entity or User Party has liability insurance, according to the current agreement and binding policies, the RA has a contractual obligation to "correctly identify and authenticate the Applicant and, if applicable, the corresponding Entity", and in virtue of this must respond to Camerfirma in the event of breach.

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

The same responsibilities are assumed by the RA in virtue of breaches of the delegated entities such as points of physical verification (PVP), without prejudice to their right to contest them.

9.6.3 Subscriber representations and warranties

9.6.3.1 Signatory/Subscriber

Signatory/Subscriber will be obliged to comply with the provisions of current regulations and in addition to:

- Use the certificate as established in this CPS and in the applicable Certification Policies.
- Respect the provisions of the documents signed with Camerfirma and the RA.
- Inform as soon as possible of the existence of any cause of suspension / revocation.

- Notify any inaccuracy or change in the data provided for the creation of the certificate during its validity period.
- Do not use the private key nor the certificate from the moment it was requested by Camerfirma or the RA because suspension or revocation, or once the period of validity of the certificate has expired.
- Make use of the digital certificate with the nature of personal and non-transferable and, therefore, assume responsibility for any action that is carried out in contravention of this obligation, as well as meet the obligations that are specific to the regulations applicable to said digital certifications.
- Authorize Camerfirma to process the personal data contained in the certificates, in connection with the purposes of the electronic relationship and, in any case, to comply with the legal obligations of certificate verification.
- Assure that all the information included, by any means, the certificate application and in the same certificate is accurate, complete for the purpose of the certificate and is updated at all times.
- Immediately inform the corresponding certification service provider of any inaccuracy in the detected certificate once it has been issued, as well as of the changes that occur in the information provided by the issuance of the certificate.
- In the case of certificates in a material device, in the event that it loses possession, bring it to the attention of the entity that issued it in the shortest possible time and, in any case, within 24 hours after the production of the aforementioned circumstance, regardless of the specific event that originated it or the actions it may eventually exercise.
- Not to use the private key, the electronic certificate or any other technical support delivered by the corresponding certification service provider to carry out any transaction prohibited by applicable law.

In the case of qualified certificates, the subscriber or the certificate holder must use the key pair exclusively for the creation of electronic signatures or stamps and in accordance with any other limitations that may be notified.

Likewise, it must be especially diligent in the custody of its private key and its secure signature creation device, in order to avoid unauthorized uses.

If the subscriber generates his own keys, he is obliged to:

- Generate your subscriber keys using an algorithm recognized as acceptable for the electronic signature, if applicable, or the electronic seal, where appropriate qualified.
- Create the keys within the signature or seal creation device, using a secure device when appropriate.
- Use key lengths and algorithms recognized as acceptable for the electronic signature, if necessary qualified, or the electronic seal, if applicable qualified.

9.6.3.2 Certificate applicant

The Applicant (either directly or through an authorized third party) of a certificate will be required to comply with the provisions of the regulations and in addition to:

- Provide the AR with the necessary information to make a correct identification.
- Guarantee the accuracy and veracity of the information provided.
- Notify any change in the data provided for the creation of the certificate during its validity period.
- Protect your private key diligently.

9.6.3.3 Entity

In the case of certificates involving a business relationship, the Entity undertakes to request suspension/revocation of the certificate from the RA when the Subject/Signatory ends its business relationship with the organization.

9.6.4 Relying party representations and warranties

The User Party undertakes to comply with legal provisions and to:

- Check the validity of the certificates before undertaking any transaction based on them. Camerfirma has established various channels for this verification, such as access to revocation lists or online query services such as OCSP, all of which are described on Camerfirma’s website.
- Know and abide by the guarantees, limits and responsibilities applicable to the acceptance and use of the certificates you rely on, and agree to abide by them. In the certificates of Representative of a Legal Person (or entity without legal personality) for Proxies that imply a representation relationship based on a special power of attorney or private document with limited powers, third parties must check the limits of such powers.
- Check the validity of the qualification of a signature associated with a certificate issued by Camerfirma by verifying that the certification authority that issued the certificate is published in the trust list of the corresponding national supervisor.

9.6.5 Representations and warranties of other participants

No stipulation

9.7. Disclaimers of warranties

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

- Not having provided the right information, initially or later as a result of changes to the circumstances described in the digital certificate, when the certification service provider has not been able to detect the inaccuracy of the data.
- Having acted negligently in terms of storing the data used to create the signature and keeping it confidential;
- Not having requested the suspension or revocation of the digital certificate data in the event of doubts raised over their storage or confidentiality;
- Having used the signature once the digital certificate has expired;
- Exceeding the limits established in the digital certificate.
- Actions attributable to the User Party, if this party acts negligently, that is, when it does not check or heed the restrictions established in the certificate in relation to allowed use and limited amount of transactions, or when it does not consider the certificate’s validity situation.
- Damages caused to the Subject or trusting third parties due to the inaccuracy of the data contained in the digital certificate, if this has been proven via a public document registered in a public register, if required.
- An inadequate or fraudulent use of the certificate in case the Subject / Holder has assigned it or authorized its use in favor of a third person by virtue of a legal transaction such as the mandate or empowerment, being the sole responsibility of the Subject / Holder the control of the keys associated with your certificate.

Camerfirma and the RAs are not liable in any way in the event of any of the following circumstances:

- Warfare, natural disasters or any other case of Force Majeure.
- The use of certificates in breach of current law and the Certification Policies.
- Improper or fraudulent use of 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 content of messages or documents signed or encrypted digitally.
- Failure to retrieve encrypted documents with the Subject’s public key.

9.8. Limitations of liability

The monetary limit of the transaction value is expressed in the final entity's certificate by including the extension "*qcStatements*", (OID 1.3.6.1.5.5.7.1.3), as defined in RFC 3039. The monetary value expression shall be in keeping with section 5.2.2 of standard TS 101 862 of the ETSI (European Telecommunications Standards Institute, www.etsi.org).

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

9.9. Indemnities

See section 9.2

9.10. Term and Termination

9.10.1 Term

See section 5.8

9.10.2 Termination

See section 5.8

9.10.3 Effect of termination and survival

See section 5.8

9.11. Individual notices and communications with participants

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

9.12. Amendments

9.12.1 Procedure for amendment

The CA reserves the right to modify this document for technical reasons or to reflect any changes in the procedures that have occurred due to legal, regulatory requirements (eIDAS, CA/B Forum, National Supervisory Bodies, etc.) or as a result of the optimization of the work cycle. Each new version of this CPS replaces all previous versions, which remain, however, applicable to the certificates issued while those versions were in force and until the first expiration date of those certificates. At least one annual update will be published. These updates will be reflected in the version box at the beginning of the document.

Changes that can be made to this CPS do not require notification except that it directly affects the rights of the subscriber, in which case they may submit their comments to the organization's policy administration within 15 days following the publication.

9.12.2 Notification mechanism and period

9.12.2.1 List of aspects

Any aspect of this CPS can be changed without notice.

9.12.2.2 Notification method

Any proposed changes to this policy are published immediately on Camerfirma’s website

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

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

Changes to this document are communicated to those third party bodies and companies that issue certificates under this PSC as well as to the relevant auditors. In particular, changes to this PSC shall be notified to the National Supervisory Bodies:

- Spain: Ministerio de Economía y Empresa (Ministry of Economy and Enterprise) or the ministry in charge of the supervision of trustworthy service providers at that time.

9.12.2.3 Period for comments

The affected Subjects/Signatories and Trusted Third Parties can submit their comments to the policy management organization within 15 days following receipt of notice. The Policies state 15 days

9.12.2.4 Comment processing system

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

9.12.3 Circumstances under which OID must be changed

Not stipulated

9.13. Dispute resolution procedure

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

9.14. Governing law

Camerfirma is obliged to fulfil the requirements established within **current Spanish and European Union law as** the trading company providing digital certification services (hereinafter, regulations or current law). This law is defined in the internal document “Compliance with legal requirements"

9.15. Compliance with applicable law

See section 9.14

9.16. Miscellaneous provisions

9.16.1 Entire agreement

The Signers and third parties that rely on the Certificates assume in their entirety the content of this Certification Practices and Policy Statement.

9.16.2 Assignment

Parties to this CPS may not assign any of their rights or obligations under this CPS or applicable agreements without the written consent of Camerfirma

9.16.3 Severability

Should individual provisions of this CPS prove to be ineffective or incomplete, this shall be without prejudice to the effectiveness of all other provisions.
The ineffective provision will be replaced by an effective provision deemed as most closely reflecting the sense and purpose of the ineffective provision. In the case of incomplete provisions, amendment will be agreed as deemed to correspond to what would have reasonably been agreed upon in line with the sense and purposes of this CPS, had the matter been considered beforehand.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Camerfirma may seek indemnification and attorneys' fees from a party for damages, losses and expenses related to that party's conduct. Camerfirma’s failure to enforce a provision of this CPS does not waive Camerfirma's right to enforce the same provisions later or right to enforce any other provisions of this CPS. To be effective any waivers must be in writing and signed by Camerfirma.

9.16.5 Force majeure

Force Majeure clauses, if existing, are included in the "Subscriber Agreement".

9.17. Other Provisions

9.17.1 Policy publication and copy

An electronic copy of this CPS is available at:

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

9.17.2 CPS approval procedures

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

AC Camerfirma publishes each new version on its website. The CPS is published in PDF format digitally signed by AC Camerfirma SA management.

APPENDIX I: document history

Oct 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
Jun 2006	V3	Amendment to adapt the document to latest changes and to ISO17799. This document is valid as an LOPD (Data Protection Act) security document and as a Security document.
May 2007	V3.1	Expiry of certificates With Power of Attorney and Without Power of Attorney
Dec 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.
Jul 2008	V3.1.3	Inclusion of CA Corporate Server EV. Changes requested by E&Y for WEBTRUST audit
Jul 2008	V3.1.4	Inclusion of section on applicable legal regulations. Changes requested by E&Y for WEBTRUST audit
Jun 2009	V3.2	Complete review of wording, inclusion of EV certificates. Inclusion of OID RACER. Information about the new ROOT 2008 passwords. Civil Servant Certificate according to the development of Law 11/2007 LAECSP. Comments on validating the title-holder in the corporate digital seal. Signing of OCSP certificates by CA. Monthly validation of EV certificates.
Feb 2010	V3.2.1	Inclusion of the new intermediate CA for Public Administrations (point 1.2.1.1 point 5) Improved description of EV certificate issue process, required by Mozilla. General review. Amended description of the person responsible for the certificate (points 1.4.8 and 2.1.3). Corrections to CRL issue (point 2.6.2) Corrections to registration of CA Public Administrations (point 6.1.1) Add reference to HSM nCipher (points 6.1.8 and 6.2) Amendment 4.8. Amendment to 8.2.1
Feb 2011	V3.2.2	Review of E&Y WebTrust renovation audit process
Mar 2011	V3.2.3	Improved description of the definition of responsibilities of the parties involved in the certification system, especially Camerfirma and the RAs. 2.2. 2.5.5 Returns policy 3.1.8 Inclusion of authorization in seal and code signing certificates. 4.5.4 Deletion of the revocation via SMS, which is no longer used. 5.2.2 Double validation of EV requests. Amendment of links to information on Camerfirma's web site.
Sep 2011	V3.2.4	Change to profile of field 1.3.6.1.4.1.17326.30.3 organization's identification document number. The first two characters that denote the country are deleted in the individual, power of representation, power of attorney, encryption and electronic invoicing profiles.
Mar 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. Inclusion 3.1.4.1

Jun 2015	V3.2.7	General review. Changes to time stamp procedures Changes to the SSL issue process. Changes of address for the links on the WEB due to changing content manager. Correction in the table of contents. Informa has been added as a source of information for issuing component certificates. Self-Employed people have been added as applicants for component certificates. Review of seal and code signing process. Inclusion of the SubCA certificate issuing for third parties, either with internal or external resources. The hierarchy of the Government of Andorra has been added in Chambersign Global Root. CGCOM Outdated certificate procedure for Vodafone mobile phones deleted. (4.3.2.3) Explanations have been added for issuing SAN certificates. 3.1.8.2.1 / 3.1.8.2.5 Centralized management of HSM passwords added. Corrections of WebTrust 2015.
Sep 2015	v.3.2.8	Modification INDECOPI (Peru Supervisor Body), 4.8.2 Causes of revocation: NEW: Signature resolution of the competent administrative or judicial authority.
Dec 2015	v.3.2.8	Text correction 6.2 about private key protection. Add Codesign OID.
Jul 2016	V3.2.9	Substitution of certificates of legal person for certificates of physical representation and electronic seals.
Mar 2018	v.3.3	1.2 clarification on the alignment of these practices with the Baseline Requirement of CA / B FORUM. 3.1.8.3.1 Incorporation of CAA checking in the validation process for Server certificates according to RFC 6844. 4.8.3 Revocation by third parties. Revocation in case of incorrect issuance (CA / BFORUM requirement). 1.5.4 Domain check delegation. 1.2.1.1 No test certificates for SSL/TSL
May 2018	V3.3.1	Adaptation of the CPS document structure according to the RFC3647 3.2.3.5 Other documents accepted to prove the link between the owner of the domain and the certificate holder. 9.1.5 Refund policy modification. 9.4 Update of the privacy clause of personal information according to European RGPD 9.7 Exemption of responsibility of the CA and AR in case of delegation of the certificate to a third party
Sep 2018	V3.3.2	Change of order, denomination and development in different points to meet RFC3647 Point '9.12.1 Procedure for amendment' is developed
Sep 2018	V3.3.3	3.2.5 Proof of relationship, the domain validation will be done by one of the methods accepted by CA/B Forum Declaration of the Guidelines for The Issue And Management Of Extended Validation Certificates version prepared by the CA/B Forum with which these CPS are aligned.
Sep 2018	V3.3.4	Minor changes in document style 3.2.5.1 Proof of relationship, Explicit statement of the methods used. 3.2.3 Incorporation of the control verification procedure on the applicant's email account. 4.2.1 The CAA checks previously reported in 3.2.5.2 are included 4.4.3, 6.4.1, 6.4.2, 7.1.6, 9.4.1, 9.4.3, 9.6.1.1 and 9.6.1.2 updated to correct mismatches with the Spanish version

		9.16.4 updated 6.2.3 updated
Aug 2019	V3.3.5	Minor changes in document style. 1.1 Updating the standards on which this CPS is based to fit your scope. 1.3.5.2 Update to conform to scope. 1.3.5.4 Incorporation of Government of Andorra profiles 1.3.5.9 scope update 1.3.5.10 Incorporation of Government of Andorra certificates under the CA 'RACER' and update of scope. 1.4.1 Appropriate uses of certificates 2.2.1 Certification Policies and Practices 2.2.2 Terms and Conditions. 3.1.1, 3.3.1, 4.1.2.1, 4.1.2.3 updating the scope. 3.1.2 replacement of point name 3.1.3 This point no longer applies because no such certificates are issued. 3.1.5.1 Issuance of several natural person certificates to one holder 3.1.6 Recognition, authentication and function of trademarks and other distinctive signs 3.1.7 Name dispute procedure 3.2.1 Methods for testing private key ownership and reference to QSCD list. 3.2.2.1 Identity 3.2.3 Identifying the identity of an individual 3.2.2.5 IP url record 3.2.5.1 Inclusion of identification of Government of Andorra certificates and adjustment of scope. 3.4 Identification and authentication of a revocation request 4.1.2.4 removal of policy reference 4.1.2.5 Crosscertification notes 4.2.2 clarification delivery of documentation and WS access 4.2.3 Deadline SubCAs not stipulated 4.3.1.3 Authenticated WS requests. 4.5.2, 4.6.1, 4.6.3, 4.6.7, 4.8, 4.9, 4.9.1, 4.9.2, 4.9.3, 4.9.6, 4.9.9, 4.9.10, 4.9.13, 4.12.1, 5.1.2, 5.2.1, 5.2.2, 5.3,5.3.7,5.3.8, 5.4.1, 5.4. 2, 5.4.3, 5.4.4, 5.4.5, 5.4.8, 5.5.1, 5.5.2, 5.5.3, 5.5.4, 5.7, 5.8, 6.1.1, 6.1.1.1, 6.1.4, 6.2.1.1, 6.2.1.2, 6.2.4, 6.2.5, 6.2.6, 6.2.8, 6.2.9, 6. 2.10, 6.2.11, 6.3.2, 6.4.1,6.4.2, 6.6.1, 6.7, 7.1, 7.1.2 7.1.4, 7.1.5, 7.1.6, 7.1.7, 7.1.9, 7.2, 7.2.2, 8, 8.1.1, 8.1.3, 8.2, 8.3, 8.4, 9.1.2, 9. 1.3, 9.6.1.1, 9.6.2, 9.6.3.1, 9.6.3.2, 9.3.3.3, 9.6.4, 9.9, 9.11, 9.12.2.2, 9.17.1, 9.17.2 various updates to adapt to new scope