CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICIES

CAMERFIRMA 2021

Version 1.0.0

Authors: Juan Ángel Martín (Compliance Consultant)

Revised by: Andrés Vázquez (Head of Compliance)
France Vidal (Head of Legal)

Approved by (PA): France Vidal (Head of Legal)

Document valid only in digital format digitally signed by the Policy Authority.

This document can be obtained from the website address https://policy2021.camerfirma.com

Language: **English**

X2392871C FRANCE MARIE SYLVIA VIDAL (C:A82743287)

X2392871C
FRANCE MARIE SYLVIA VIDAL (C:A82743287)
2022.02.21 16:48:43 +01'00'

Table of Contents

1. INTRODUCTION

1.1. GENERAL OVERVIEW

Given that there is no unquestionable definition of the concepts of the Certification Practice Statement and Certificate Policies, Camerfirma would like to explain its stance in relation to these concepts, in accordance with IETF RFC 3647.

Certificate Policy (hereinafter, 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 CP must generally define the applicability of certificate types for certain applications that establish the same security and usage requirements.

Certification Practice Statement (hereinafter, CPS): a set of practices adopted by a Certification Authority (hereinafter, CA) for the issuance, management, revocation, and renewal or re-key of certificates. It usually contains detailed information about its certificate security, support, administration, issuing (including renewing and/or re-keying) and revoking systems, as well as the trust relationship between the Subject, the Relying Party and the CA. These may be completely comprehensible and robust documents that provide an accurate description of the services offered, detailed certificate lifecycle management procedures, etc.

These CP and CPS concepts are different, although they are still closely interrelated. A detailed CPS is not an acceptable basis for the interoperability of CAs. CPs are a better basis for common security standards and criteria.

In summary, a CP defines “which” security requirements are required for the issuance (including renewal and/or re-key) and revocation of certificates. The CPS defines “how” the security requirements established in the CP are fulfilled.

Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (hereinafter, referred to as eIDAS Regulation) defines a ‘trust service’ as an electronic service normally provided for remuneration which consist of:

(a) the creation, verification and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to these services, or

(b) the creation, verification and validation of certificates for website authentication, or

(c) the preservation of electronic signatures, seals or certificates relating to those services.

This document specifies the CPS and the CPs that AC Camerfirma SA (hereinafter, Camerfirma) has established for the creation, verification and validation of certificates related to electronic signatures, issued by Camerfirma CAs under CAMERFIRMA ROOT 2021 hierarchy, in accordance with eIDAS Regulation and based on the following standards:

Service	EN general	EN scope	Profiles/Semantics
Creation, verification and validation of certificates related to electronic signatures	EN 319 401 v2.3.1 General Policy Requirements for Trust Service Providers	EN 319 411-1 v1.3.1: Trust Service Providers issuing certificates; Part 1: General Requirements EN 319 411-2 v2.4.1: Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates	EN 319 412-1 v1.4.4: Certificate Profiles; Part 1: Overview and common data structures EN 319 412-2 v2.2.1: Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons EN 319 412-5 v2.3.1: Certificate Profiles; Part 5: QcStatements

Regarding the certificate policies to be applied in accordance with ETSI EN 319 411-1 and ETSI EN 319 411-2, the following are included in the CPs described in this document:

- General certificate policies (ETSI EN 319 411-1):

  NCP Normalized Certificate Policy.

  NCP+ Extended Normalized Certificate Policy.

- Certificate policies for EU qualified certificates (ETSI EN 319 411-2):

  QCP-n Certificate Policy for EU qualified certificates issued to natural persons. Includes all the NCP policy requirements, plus additional requirements suited to support EU qualified certificates issuance and management as specified in eIDAS Regulation. Certificates issued under these requirements are aimed to support the advanced electronic signatures based on a qualified certificate defined in articles 26 and 27 of eIDAS Regulation.

  QCP-n-qscd Certificate Policy for EU qualified certificates issued to natural persons with private key related to the certified public key in a Qualified Electronic Signature Creation Device (hereinafter, QSCD). Includes all the QCP-n policy requirements (including all the NCP+ policy requirements), plus additional provisions suited to support EU qualified certificates issuance and management as specified in eIDAS Regulation, including those specific to the QSCD provision. Certificates issued under these requirements are aimed to support qualified electronic signatures such as defined in article 3 (12) of eIDAS Regulation.

In addition, this document is compliant with the Spanish Law 6/2020 of 11 November (hereinafter, Law 6/2020) concerning some aspects of electronic trust services.

The document is structured in accordance with IETF RFC 3647.

1.2. DOCUMENT NAME AND IDENTIFICATION

Name: CPS and CPs Camerfirma 2021

Description: Certification Practice Statement and Certificate Policies for Camerfirma CAs under CAMERFIRMA ROOT 2021 hierarchy

Version: See homepage

OIDs
- 1.3.6.1.4.1.17326.10.21.1 (CPS)
- 1.3.6.1.4.1.17326.10.21.1.2.1 (CP QUALIFIED CORPORATE CERTIFICATE - QCP-n-qscd in QSCD SmartCard or Token)
- 1.3.6.1.4.1.17326.10.21.1.2.3 (CP QUALIFIED CORPORATE CERTIFICATE - QCP-n-qscd in QSCD Cloud)
- 1.3.6.1.4.1.17326.10.21.1.3.1 (CP QUALIFIED CERTIFICATE FOR A LEGAL REPRESENTATIVE OF A LEGAL ENTITY - QCP-n-qscd in QSCD SmartCard or Token)
- 1.3.6.1.4.1.17326.10.21.1.3.3 (CP QUALIFIED CERTIFICATE FOR A LEGAL REPRESENTATIVE OF A LEGAL ENTITY - QCP-n-qscd in QSCD Cloud)
- 1.3.6.1.4.1.17326.10.21.1.4.1 (CP QUALIFIED CERTIFICATE FOR A LEGAL REPRESENTATIVE OF A NON-LEGAL ENTITY - QCP-n-qscd in QSCD SmartCard or Token)
- 1.3.6.1.4.1.17326.10.21.1.4.3 (CP QUALIFIED CERTIFICATE FOR A LEGAL REPRESENTATIVE OF A NON-LEGAL ENTITY - QCP-n-qscd in QSCD Cloud)
- 1.3.6.1.4.1.17326.10.21.1.5.1 (CP QUALIFIED CERTIFICATE FOR A VOLUNTARY REPRESENTATIVE OF A LEGAL ENTITY BEFORE THE PUBLIC ADMINISTRATIONS - QCP-n-qscd in QSCD SmartCard or Token)
- 1.3.6.1.4.1.17326.10.21.1.5.3 (CP QUALIFIED CERTIFICATE FOR A VOLUNTARY REPRESENTATIVE OF A LEGAL ENTITY BEFORE THE PUBLIC ADMINISTRATIONS - QCP-n-qscd in QSCD Cloud)

- 1.3.6.1.4.1.17326.10.21.1.6.1 (CP QUALIFIED CERTIFICATE FOR A VOLUNTARY REPRESENTATIVE OF A NON-LEGAL ENTITY BEFORE THE PUBLIC ADMINISTRATIONS - QCP-n-qscd in QSCD SmartCard or Token)
- 1.3.6.1.4.1.17326.10.21.1.6.3 (CP QUALIFIED CERTIFICATE FOR A VOLUNTARY REPRESENTATIVE OF A NON-LEGAL ENTITY BEFORE THE PUBLIC ADMINISTRATIONS - QCP-n-qscd in QSCD Cloud)
- 1.3.6.1.4.1.17326.10.21.1.7.1 (CP QUALIFIED CERTIFICATE FOR A SPECIAL REPRESENTATIVE OF A LEGAL ENTITY - QCP-n-qscd in QSCD SmartCard or Token)
- 1.3.6.1.4.1.17326.10.21.1.7.3 (CP QUALIFIED CERTIFICATE FOR A SPECIAL REPRESENTATIVE OF A LEGAL ENTITY - QCP-n-qscd in QSCD Cloud)
- 1.3.6.1.4.1.17326.10.21.1.8.1 (CP QUALIFIED CERTIFICATE FOR A SPECIAL REPRESENTATIVE OF A NON-LEGAL ENTITY - QCP-n-qscd in QSCD SmartCard or Token)
- 1.3.6.1.4.1.17326.10.21.1.8.3 (CP QUALIFIED CERTIFICATE FOR A SPECIAL REPRESENTATIVE OF A NON-LEGAL ENTITY - QCP-n-qscd in QSCD Cloud)

Location: https://policy21.camerfirma.com

1.3. PKI PARTICIPANTS

1.3.1. CERTIFICATION AUTHORITIES (CAS)

A CA is a component of a PKI responsible for issuing and managing digital certificates. A CA is a type of Trusted Service Provider (TSP) that issues digital certificates. It acts as the trusted third party between the Subject and the Relying Party in digital transactions, associating a specific public key with the Subject. The CA has the ultimate responsibility in the provision of certification services.

The issuing CA is identified in the *Issuer* field of every digital certificate.

Under this CPS, a CA belongs to the legal person specified in the organization attribute (O) of the *Issuer* field of the digital certificates issued by this CA.

Under this CPS, Camerfirma is acting as CAs with the following corporate data:

Corporate name: AC CAMERFIRMA, S.A.

Tax number (NIF): A82743287

Headquarter: calle Ribera del Loira 12 - 28042 Madrid

Telephone: +34 91 344 37 43

Email: ca@camerfirma.com

Webpage: https://www.camerfirma.com

Since May of 2018, Camerfirma is owned by the Italian company InfoCert, S.p.A., subject to the management and coordination of TINEXTA, S.p.A. (webpage: https://www.infocert.it).

A CA uses Registration Authorities (hereinafter, RA) for the purpose of checking and storage of end entity digital certificates content documentation. Under current CPS, The CAs can carry out the RAs' work at any time.

A TSP can incorporate one or more CA hierarchies. A CA hierarchy includes a Root CA and one or more Intermediate CAs (also known as Subordinate CAs).

The use of CA hierarchies reduces the risks involved in issuing certificates and organising them in the different CAs. The Intermediate CAs keys are managed in a more agile online environment, while the Root CA keys are managed in a more secure offline environment.

An Intermediate CA obtains a certificate from the Root CA to issue end entity certificates or other Intermediate CA certificates. The number of intermediate CAs allowed under a Root or Intermediate CA is specified in the Basic Constraints (pathLenConstraint) extension of the CA's certificate.

The following section describes the CA hierarchy that Camerfirma manages as owner (either directly or through subsidiaries) under this CPS. In the case of Intermediate CA owned by another organization, this CPS will refer its existence within the corresponding hierarchy due to its subjection to the Root CA, but it will be governed by its own CPS.

As a general feature, the names of the CAs in the certificates issued to them incorporate the year of certificate issuance. For example, the name of the CA can change to include the year of a new certificate issuance at the end of the name, although the characteristics will remain the same, unless otherwise stated in this CPS.

Under this CPS, Camerfirma manages the following CA hierarchy:

- CAMERFIRMA ROOT 2021

1.3.1.1. CAMERFIRMA ROOT 2021 HIERARCHY

This CA hierarchy is designed to develop a trusted network, with the ultimate aim of issuing digital certificates within the European Union, and in which the RAs are managed by the Spanish Chambers of Commerce, Industry and Navigation or other public or private entities.

The identification details for the Root CA certificate of this hierarchy are:

CN: CAMERFIRMA ROOT 2021

Valid from (UTC Time): 19/10/2021 12:26:35

Valid until (UTC Time): 13/10/2045 12:26:35

Serial Number: 34 61 2C A9 B6 C3 7A 12 FE 65 50 A0 6B 28 EE EC EE BA F3 E4

X509v3 Subject Key Identifier: 51 11 32 7A 10 D0 D8 8C 4C 09 84 97 B1 A9 3E B2 54 BA 87 C9

Hash SHA-1: 33 9F 6E F0 37 AA EE BA A0 CE 54 80 06 02 DD FB 18 6C 1C EE

Hash SHA-256: AD FC 94 10 EE 0D 10 91 EE FD 5C DD FA E5 65 1E 3B 1D 66 B6 9C 0D AB C5 9E 33 91 B3 58 5A 53 8E

The scheme of Intermediate Certification Authorities issuing digital certificates under this hierarchy is:

CAMERFIRMA ROOT 2021	
AC CAMERFIRMA QUALIFIED CERTIFICATES – 2021	
1.3.6.1.4.1.17326.10.21.1.2.1 [Camerfirma] 0.4.0.194112.1.2 [eIDAS QCP-n-qscd]	QUALIFIED CORPORATE CERTIFICATE – QCP-n-qscd in QSCD SmartCard or Token
1.3.6.1.4.1.17326.10.21.1.2.3 [Camerfirma] 0.4.0.194112.1.2 [eIDAS QCP-n-qscd]	QUALIFIED CORPORATE CERTIFICATE – QCP-n-qscd in QSCD Cloud

1.3.6.1.4.1.17326.10.21.1.3.1 [Camerfirma] 2.21.724.1.3.5.8 [Spanish Public Administration requirement] 0.4.0.194112.1.2 [eIDAS QCP-n-qscd]	QUALIFIED CERTIFICATE FOR A LEGAL REPRESENTATIVE OF A LEGAL ENTITY – QCP-n-qscd in QSCD SmartCard or Token
1.3.6.1.4.1.17326.10.21.1.3.3 [Camerfirma] 2.21.724.1.3.5.8 [Spanish Public Administration requirement] 0.4.0.194112.1.2 [eIDAS QCP-n-qscd]	QUALIFIED CERTIFICATE FOR A LEGAL REPRESENTATIVE OF A LEGAL ENTITY – QCP-n-qscd in QSCD Cloud
1.3.6.1.4.1.17326.10.21.1.4.1 [Camerfirma] 2.21.724.1.3.5.9 [Spanish Public Administration requirement] 0.4.0.194112.1.2 [eIDAS QCP-n-qscd]	QUALIFIED CERTIFICATE FOR A LEGAL REPRESENTATIVE OF A NON-LEGAL ENTITY – QCP-n-qscd in QSCD SmartCard or Token
1.3.6.1.4.1.17326.10.21.1.4.3 [Camerfirma] 2.21.724.1.3.5.9 [Spanish Public Administration requirement] 0.4.0.194112.1.2 [eIDAS QCP-n-qscd]	QUALIFIED CERTIFICATE FOR A LEGAL REPRESENTATIVE OF A NON-LEGAL ENTITY – QCP-n-qscd in QSCD Cloud
1.3.6.1.4.1.17326.10.21.1.5.1 [Camerfirma] 2.21.724.1.3.5.8 [Spanish Public Administration requirement] 0.4.0.194112.1.2 [eIDAS QCP-n-qscd]	QUALIFIED CERTIFICATE FOR A VOLUNTARY REPRESENTATIVE OF A LEGAL ENTITY BEFORE THE PUBLIC ADMINISTRATIONS – QCP-n-qscd in QSCD SmartCard or Token
1.3.6.1.4.1.17326.10.21.1.5.3 [Camerfirma] 2.21.724.1.3.5.8 [Spanish Public Administration requirement] 0.4.0.194112.1.2 [eIDAS QCP-n-qscd]	QUALIFIED CERTIFICATE FOR A VOLUNTARY REPRESENTATIVE OF A LEGAL ENTITY BEFORE THE PUBLIC ADMINISTRATIONS – QCP-n-qscd in QSCD Cloud
1.3.6.1.4.1.17326.10.21.1.6.1 [Camerfirma] 2.21.724.1.3.5.9 [Spanish Public Administration requirement] 0.4.0.194112.1.2 [eIDAS QCP-n-qscd]	QUALIFIED CERTIFICATE FOR A VOLUNTARY REPRESENTATIVE OF A NON-LEGAL ENTITY BEFORE THE PUBLIC ADMINISTRATIONS – QCP-n-qscd in QSCD SmartCard or Token
1.3.6.1.4.1.17326.10.21.1.6.3 [Camerfirma] 2.21.724.1.3.5.9 [Spanish Public Administration requirement] 0.4.0.194112.1.2 [eIDAS QCP-n-qscd]	QUALIFIED CERTIFICATE FOR A VOLUNTARY REPRESENTATIVE OF A NON-LEGAL ENTITY BEFORE THE PUBLIC ADMINISTRATIONS – QCP-n-qscd in QSCD Cloud
1.3.6.1.4.1.17326.10.21.1.7.1 [Camerfirma] 0.4.0.194112.1.2 [eIDAS QCP-n-qscd]	QUALIFIED CERTIFICATE FOR A SPECIAL REPRESENTATIVE OF A LEGAL ENTITY – QCP-n-qscd in QSCD SmartCard or Token

1.3.6.1.4.1.17326.10.21.1.7.3 [Camerfirma] 0.4.0.194112.1.2 [eIDAS QCP-n-qscd]	QUALIFIED CERTIFICATE FOR A SPECIAL REPRESENTATIVE OF A LEGAL ENTITY – QCP-n-qscd in QSCD Cloud
1.3.6.1.4.1.17326.10.21.1.8.1 [Camerfirma] 0.4.0.194112.1.2 [eIDAS QCP-n-qscd]	QUALIFIED CERTIFICATE FOR A SPECIAL REPRESENTATIVE OF A NON-LEGAL ENTITY – QCP-n-qscd in QSCD SmartCard or Token
1.3.6.1.4.1.17326.10.21.1.8.3 [Camerfirma] 0.4.0.194112.1.2 [eIDAS QCP-n-qscd]	QUALIFIED CERTIFICATE FOR A SPECIAL REPRESENTATIVE OF A NON-LEGAL ENTITY – QCP-n-qscd in QSCD Cloud

All the Camerfirma CA certificates can issue OCSP responder certificates to be used to sign the OCSP service's responses regarding the status of the certificates issued by the CAs. The OID of OCSP responder certificates issued by all the Camerfirma CAs is 1.3.6.1.4.1.17326.10.21.0.1

1.3.1.1.1. AC CAMERFIRMA QUALIFIED CERTIFICATES – 2021

AC CAMERFIRMA QUALIFIED CERTIFICATES – 2021 is a multi-policy Intermediate CA, that may issue qualified certificates for natural and legal persons (at present, only for natural persons) within the EU, and in accordance with the requirements of the eIDAS Regulation and Law 6/2020.

The identification details for this CA certificate (issued by the Root CA of the CAMERFIRMA ROOT 2021 hierarchy):

CN: AC CAMERFIRMA QUALIFIED CERTIFICATES – 2021

Valid from (UTC Time): 20/10/2021 15:12:16

Valid until (UTC Time): 16/10/2037 15:12:16

Serial Number: 1C 20 0D 92 11 23 B8 98 38 0F C2 B9 24 19 BB A9 9B 94 C2 C2

X509v3 Subject Key Identifier: C7 6F 2D C4 10 8A 6E DD F3 11 65 69 C6 4A 43 7B

Hash SHA-1: 2E 0F 6F 10 E6 14 5E 50 57 FC 03 B2 53 C5 00 6E E0 6D 19 EE

Hash SHA-256: 4D 18 7D 4E 5B BA 7B BA D4 22 B7 5B EF B4 DC B2 17 9D 1C CD 11 5A 18 D2 C8 35 0F FF AC 31 6B 34

The end entity certificates issued by this CA are intended for:

1.3.1.1.1.1. NATURAL PERSONS WITH A BUSINESS RELATIONSHIP WITH AN ENTITY

1.3.1.1.1.1.1. QUALIFIED CORPORATE CERTIFICATE – QCP-N-QSCD

This certificate identifies a natural person (Holder/Subject/Signatory) and determines as specific attributes, the type of contractual relationship (employment, commercial, institution, etc.) between a natural person (Holder/Subject/Signatory) and an Entity (certificate organization field).

1.3.1.1.1.1.2. QUALIFIED CERTIFICATE FOR A LEGAL REPRESENTATIVE OF A LEGAL ENTITY – QCP-N-QSCD.

This certificate identifies a natural person (Holder/Subject/Signatory) and determines as specific attributes, his/her status as a legal representative or representative with General and full Power of Attorney, with the capability to act on behalf of a Legal Entity.

It is aimed at legal representatives of entities with legal personality such as Sole Administrator, Joint Administrator, Director-Delegate, CEO, etc., and empowered persons with voluntary General Power of Attorneys that includes full powers of representation (similar to those of a legal representative) that allows them to act both in the field of relations and procedures with the Public Administrations (authentication and signature uses) and in the field of contracting goods or services or relating to the ordinary business of the organization (signature uses).

The jointly legal representatives or the jointly empowered persons by a General Power of Attorneys who wishes to apply this certificate must hold powers that include at least, the jointly and severally power to represent the Legal Entity to carry out relations and procedures with Public Administrations.

In any case, the certificate Holder/Subject/Signatory is in charge of using it in accordance with its Powers and the Relying Party to verify its content and scope.

1.3.1.1.1.1.3. QUALIFIED CERTIFICATE FOR A LEGAL REPRESENTATIVE OF A NON-LEGAL ENTITY – QCP-N-QSCD.

This certificate identifies a natural person (Holder/Subject/Signatory) and determines as specific attributes, his/her status as legal representative or representative with General and full Power of Attorney, with capability to act on behalf of a Non-legal Entity.

It is aimed at legal representatives of Non-legal Entities such as Sole Administrator, Joint Administrator, Director/Manager, President of Property Owners, etc., and empowered persons with voluntary General Power of Attorneys that includes full powers of representation (similar to those of a legal representative) that allows them to act both in the field of relations and procedures with Public Administrations (authentication and signature uses) and in the field of contracting goods or services or relating the ordinary business of the organization (signature uses).

The jointly legal representatives or the jointly empowered persons by a General Power of Attorneys who want to apply this certificate must hold powers that include at least, the jointly and severally power to represent the Non-legal Entity to carry out relations and procedures with Public Administrations.

In any case, the certificate Holder/Subject/Signatory is in charge of using it in accordance with its Powers and the Relying Party to verify its content and scope.

1.3.1.1.1.1.4. QUALIFIED CERTIFICATE FOR A VOLUNTARY REPRESENTATIVE OF A LEGAL ENTITY BEFORE THE PUBLIC ADMINISTRATIONS – QCP-N-QSCD.

The purpose of this certificate is to identify a natural person (Holder/Subject/Signatory) and determines as specific attributes, his/her capability to represent a legal Entity in the scope of the Entity's relationship with the Public Administrations (authentication and signature uses).

It is aimed at empowered persons with General Power of Attorneys or Specific Power of Attorneys which includes at least faculties that allows them to request electronic certificates to carry out, on behalf of the Legal entity, actions and procedures with Public Administrations that require the use of the electronic signature or electronic certificate.

The jointly legal representatives or the jointly empowered persons by General Power of Attorneys or Specific Power of Attorneys who want to apply this certificate as long as their powers include at least the jointly and severally power to represent the Legal entity to carry out relationships and procedures before Public Administrations. Alternatively, they can provide a Specific Power of attorney signed by all the jointly empowered persons in favor of one of them.

In any case, the certificate Holder/Subject/Signatory is in charge of using it in accordance with its Powers and the Relying Party to verify its content and scope.

1.3.1.1.1.1.5. QUALIFIED CERTIFICATE FOR A VOLUNTARY REPRESENTATIVE OF A NON-LEGAL ENTITY BEFORE THE PUBLIC ADMINISTRATIONS – QCP-N-QSCD.

The purpose of this certificate is to identify a natural person (Holder/Subject/Signatory) and determines as specific attributes, his/her capability to represent a Non-legal Entity in the field of relationship of the Entity with Public Administration (authentication and signature uses).

It is aimed at empowered persons with General Power of Attorneys or Specific Power of Attorneys which includes at least faculties that enable them to request electronic certificates to perform on behalf of the non-legal Entity actions and procedures with Public Administrations that require the use of the electronic signature or electronic certificate.

The jointly legal representatives or the jointly empowered persons by General Power of Attorneys or Specific Power of Attorneys who want to apply this certificate as long as their powers include at least the jointly and severally power to represent the Non-legal Entity to carry out relationships and procedures before Public Administrations. Alternatively, they can provide a Specific Power of Attorney, or a reliable document signed by all the jointly empowered persons in favor of one of them.

In any case, the certificate Holder/Subject/Signatory is in charge of using it in accordance with its Powers and the Relying Party to verify its content and scope.

1.3.1.1.1.1.6. QUALIFIED CERTIFICATE FOR A SPECIAL REPRESENTATIVE OF A LEGAL ENTITY – QCP-N-QSCD.

This certificate identifies a natural person (Holder/Subject/Signatory) and determines as specific attributes, his/her capability to act on behalf of a legal Entity only for certain powers or faculties framed in his/her function/department (signature uses).

This certificate is not recommended for authentication uses on Public Administration platforms because of the implicit limitation of the powers whose accurate scope the Relying Party cannot know.

Special jointly empowered persons who want to apply this certificate if they provide a notarized Power of Attorney, or a document signed by all the joint authorized representatives in favor of one of them.

In any case, the certificate Holder/Subject/Signatory is in charge of using it in accordance with its Powers and the Relying Party to verify its content and scope.

1.3.1.1.1.1.7. QUALIFIED CERTIFICATE FOR A SPECIAL REPRESENTATIVE OF A NON-LEGAL ENTITY – QCP-N-QSCD.

This certificate identifies a natural person (Holder/Subject/Signatory) and determines as specific attributes, his/her capability to act on behalf of a Non-legal Entity only for certain powers or faculties framed in his/her function / department (signatures uses).

This certificate is not recommended for authentication uses on Public Administration platforms because of the implicit limitation of the powers whose accurate scope the Relying Party cannot know.

Special jointly empowered persons who want to apply this certificate if they provide a notarized Power of Attorney, or a document signed by all the joint authorized representatives in favor of one of them.

In any case, the certificate Holder/Subject/Signatory is in charge of using it in accordance with its Powers and the Relying Party to verify its content and scope.

1.3.1.2. ISSUING TEST CERTIFICATES

Camerfirma issues certificates with fictitious data by CAs to provide them to regulatory bodies for new certificates inspection, accreditation or registration processes, as well as to application developers to be used in the process of integration or evaluation for certificate acceptance. Camerfirma includes the following information in these certificates so that the Relying Party can clearly see that it is a test certificate without liability:

Name of the entity: [SOLO PRUEBAS]/[TEST ONLY] ENTIDAD
Entity Tax ID No.: R0599999J
Name: JUAN ANTONIO
First Surname: CÁMARA
Second Surname: ESPAÑOL
National ID No.: 00000000T
CN: [SOLO PRUEBAS]/[TEST ONLY] ...

When a process requires the issuance of a test certificate with real data, this is done only after signing a confidentiality agreement with the entity responsible for the process. In this case, the data is specific to each customer, but before the

entity name '[SOLO PRUEBAS]' or '[TEST ONLY]' always appears in order to identify at first sight that it is a test certificate without liability.

1.3.2. REGISTRATION AUTHORITIES (RAS)

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

Under current CPS, the following types of RA are recognized:

- Chambers RA: Those managed directly or under the control of a Spanish Chamber of Commerce, Industry and Navigation.
- Corporate RA: Those managed by a public organization or a private entity for distributing certificates to its employees.

For the purpose of this CPS, the following can act as RA of the intermediate CAs owned by AC Camerfirma:

- The CA.
- The Spanish Chambers of Commerce, Industry and Navigation, or the entities appointed by them. The delegated entities can carry out the registration process.
- Spanish Companies, as entities delegated by the RA of the CA or by the Spanish Chambers of Commerce, Industry and Navigation RA, to which they are contractually associated, in order to make the complete identification and registration of the Applicant, within a particular organization or demarcation. In general, the operators of these Corporate RA only manage the service in the area of their organization or demarcation, unless determined otherwise by the RA on which they depend. For example, a corporation's employees, members of a corporate group, members of a professional body.
- Entities belonging to the Spanish Public Administrations.
- Other Spanish or international legal entities or agents that have a contractual relationship with the CAs and have passed the registration processes. They are obliged to successfully complete the audits required in the agreement according to the CP. For the issuance of certificates to natural or legal persons that do not reside in Spanish territory, a legal report may be required to justify the correct compliance with the identification and registration requirements.

At the same time, RA can partially delegate to a third person/entity named Point of Physical Verification (PPV) the identification tasks:

- PPV. Point of Physical Verification that always depends on an RA. Its main mission is to identify the Applicant by a face to face method and give to the RA the evidence of the identification. The RA checked the evidence and if it's correct, validate in accordance with applicable issuance procedure.
  Sometimes, the PPVs' 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 SmartCard or Token, but a PPV can never validate the registration process and decide the certificate issuance. AC Camerfirma has drafted a relationship type document between the RA and the PPV where the functions delegated by the RA to the PPV are defined.

1.3.3. SUBSCRIBERS AND SUBJECTS/HOLDERS

Under this CPS and according to ETSI EN 319 401, the Subscriber is the legal or natural person bound by agreement with Camerfirma acting as CA to any subscriber obligations.

Under this CPS and according to ETSI EN 319 411-1, the Subject is the certificate Holder (holder of the private key associated with the public key in the certificate) and is described in the *Subject* field of the certificate.

Under this CPS and according to eIDAS Regulation, the Subject/Holder of a certificate for electronic signature is a natural person named the *Signatory*, and the Subject/Holder of a certificate for electronic seal is a legal person named the *Creator of the seal*.

Under CPs described in this document the Subject/Holder can be:

- A natural person associated with an organization.

Under CPs described in this document the Subscriber can be:

- The organization to whom the natural person Subject/Holder is associated.
- The natural person Subject/Holder.

In order to avoid a conflict of interest, Camerfirma can't be the Subscriber of electronic certificates except if it issues for itself (as a legal person) or natural persons belonging to it (as a Subject) and except cases where a third party organization running all or part of the RA tasks in order to subscribe to certificates for subjects identified in association with it. In both cases the request, validation and handle must be done according to Camerfirma defined processes.

1.3.4. RELYING PARTIES

In this document, the Relying Party is the person receiving a digital transaction carried out with a certificate issued by any of the Camerfirma CAs included in this document and who voluntarily trusts the Certificate that the CA issues.

1.3.5. OTHER PARTICIPANTS

1.3.5.1. ACCREDITATION ENTITY OR SUPERVISORY BODY

The Supervisory Body is the corresponding management entity that accepts, accredits and supervises the TSPs within a specific geographic area. Within Spain, this task is the responsibility of *Ministerio de Asuntos Económicos y Transformación Digital*, which is the competent authority depending on the Spanish State member of the European Economic Space.

The Intermediate CAs not owned by Camerfirma may be subject to legal frameworks in different countries or regions. In such cases, the Supervisory Body refers to the relevant national body.

1.3.5.2. TRUSTED SERVICE PROVIDER (TSP)

According to eIDAS Regulation, a Trusted Service Provider (TSP) is a natural person or legal person who provides one or more trust services either as a qualified or as a non-qualified trusted service provider.

According to eIDAS Regulation, a Qualified Trusted Service Provider (QTSP) is a TSP who provides one or more qualified trusted services and is granted the qualified status by the Supervisory Body.

The trusted services defined in eIDAS Regulation include:

- The creation, verification and validation of electronic signatures. Certificates relating to these services are included.
- The creation, verification and validation of electronic seals. Certificates relating to these services are included.
- The creation, verification and validation of electronic time stamps. Certificates relating to these services are included.
- Electronic registered delivery services. Certificates relating to these services are included.
- The preservation of electronic signatures, seals or certificates related to those services.

1.3.5.3. ENTITY/ORGANIZATION

Under CPS and CPs described in this document, the Entity is a public or private, individual or collective organization, recognized under the law, with which the natural person/Subject/Holder/Signatory maintains a certain relationship, as defined in the ORGANIZATION field (O) in each certificate. Depending on the case, it can be the Subscriber (section 1.3.3 or not).

1.3.5.4. APPLICANT

Under this CPS, Applicant means the Subject/Holder when this is a natural person, and means the natural person who performs the certificate application on behalf of the Subject/Holder when this is a legal person.

Under CPs described in this document, Applicant means the Subject/Holder.

1.3.5.5. RESPONSIBLE

For certificates issued to natural persons, this CPS and CPs described in this document consider the Subject/Holder to be the person Responsible for the certificate (responsible for the private key associated with the public key in the certificate).

For certificates issued to legal persons, without prejudice to the obligations of the Subject/Holder, this CPS considers the

Applicant, or a natural person authorized by the Applicant, to be the Responsible for the certificate (responsible for the private key associated with the public key in the certificate).

1.4. CERTIFICATE USAGE

1.4.1. APPROPRIATE CERTIFICATE USES

Certificates for natural or legal persons issued under these policies are used for the following purposes:

- Certificate Subject/Holder authentication.
- Electronic, advanced, or qualified signature when used with qualified electronic signature creation devices.
- Asymmetric or mixed encryption without key recovery.

1.4.2. PROHIBITED CERTIFICATE USES

Camerfirma includes information on the limitation of use in the certificate, either in standardised fields in the attributes "key usage", "basic constraints" marked as critical in the certificate and therefore mandatory for the applications that use it, or limitations in attributes such as "extended key usage", "name constraints" and/or through texts included in the "issuer's statement" field (user notice) marked as "non-critical" but mandatory for the certificate holder and user.

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

The certificates are not designed, may not be used, and are not authorised for use or resale as monitoring equipment for dangerous situations or for uses requiring fail-safe actions, such as the operation of nuclear facilities, navigation systems or aerial communication or weapons control systems, where failure could lead directly to death, personal injury or severe environmental damage.

The use of digital certificates in transactions that contravene the CP applicable to each of the Certificates, the CPS or the Terms and Conditions that the CAs sign with the RAs and with the Subscribers/Subjects is considered illegal, and the CAs are exempt from any liability due to the Signatory or third party's misuse of the certificates in accordance with current law.

Camerfirma does not have access to the data for which a certificate is used. Therefore, due to the lack of access to messages' contents, Camerfirma cannot issue any assessment regarding these contents and the Signatory is therefore responsible for the data for which the certificate is used. The Signatory is also responsible for the consequences of any use of this data contrary to the limitations and conditions established this document and in the Terms and Conditions the CAs sign with the Subject/Signatory, as well as any misuse thereof in accordance with this section or which may be interpreted as such by virtue of current legislation.

The private key of the certificates is stored by Camerfirma only for certificate in QSCD Cloud, and therefore it is not possible to recover the encrypted data with the corresponding public key in the event of loss of the certificate's private key by the certificate holder. If the holder encrypts data with the public key, he/she does so under his/her own and sole responsibility.

1.5. POLICY ADMINISTRATION

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

1.5.1. ORGANIZATION ADMINISTERING THE DOCUMENT

The drafting and revision of this document is done by the Camerfirma compliance and legal departments in collaboration with the operation and system departments.

1.5.2. CONTACT PERSON

Address: Calle Ribera del Loira, 12. Madrid (Spain)

Phone: +34 91 344 37 43

Email: compliance@camerfirma.com

Webpage: https://www.camerfirma.com

In terms of the content of this CPS and 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 https://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 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 CA hierarchies described above being responsible for the suitability of the CPS and CPs in this document.

1.5.4. CPS APPROVAL PROCEDURES

The publication of the revisions of this document must be approved by the Policy Authority that is the legal department of Camerfirma.

AC Camerfirma publishes every new version of this document on its website https://policy21.camerfirma.com. The CPS is published in PDF format electronically signed with the digital certificate of the approver.

1.6. DEFINITIONS AND ACRONYMS

1.6.1. ACRONYMS

AgID	*Agenzia per l'Italia Digitale*.
AWS	Amazon Web Services.
CA	Certification Authority.
CAB	Conformity Assessment Body.
CC	Common Criteria.
CN	Common Name.
CP	Certificate Policy.
CPS	Certification Practice Statement.
CRL	Certificate Revocation List. List of revoked certificates.
CSR	Certificate Signing Request.
DMZ	Demilitarized Zone.
DN	Distinguished Name.
DNI	National Identity Card (*Documento Nacional de Identidad*).
EAL	Evaluation Assurance Level.
EEA	European Economic Area.
eIDAS	electronic Identification, Authentication and trust Services.
EN	European Standards.

ETSI	European Telecommunications Standards Institute.
EU	European Union.
FIPS	Federal Information Processing Standard Publication.
GLONASS	Global Navigation Satellite System.
GPS	Global Positioning System.
HSM	Hardware Security Module.
HTTP	Hypertext Transfer Protocol.
IEC	International Electrotechnical Commission.
IETF	Internet Engineering Task Force.
INRIM	Italian National Institute of Metrological Research.
ISO	International Standards Organization.
ITU	International Telecommunications Union.
MPLS	Multiprotocol Label Switching.
NAS	Network-Attached Storage.
NCP	Normalized Certificate Policy.
NCP+	Extended Normalized Certificate Policy.
NIE	Foreigner Identity Number (*Número de Identidad de Extranjero*).
NTP	Network Time Protocol.
O	Organization.
OCSP	On-line Certificate Status Protocol. Protocol for accessing the status of certificates.
OID	Object Identifier.
OTP	One-time password.
PA	Policy Authority.
PadES	PDF Advanced Electronic Signatures.
PDF	Portable Document Format.
PIN	Personal Identification Number.
PKCS#10	The most common format for CSRs.
PKI	Public Key Infrastructure.

PPV	Point of Physical Verification.
QCP-n	Policy for EU Qualified Certificate issued to a natural person.
QCP-n-qscd	Policy for EU Qualified Certificate issued to a natural person where the private key and the related certificate reside on a QSCD.
QSCD	Qualified electronic Signature/Seal Creation Device.
QTSP	Qualified Trusted Service Provider.
RA	Registration Authority.
RFC	IETF Request for Comments.
RGPD	General Data Protection Regulation (EU) 2016/679.
RSA	Rivest-Shamir-Adleman. Type of encryption algorithm.
RTO/RPO	Recovery Time Objective/Recovery Point Objective.
SHA	Secure Hash Algorithm.
SSCD	Secure Signature Creation 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.
STS	Station-to-Station protocol.
TIN	Tax Identification Number.
TS	ETSI Technical Specification.
TSP	Trusted Service Provider.
UPS	Uninterruptible Power Supply.
UTC	Coordinated Universal Time.
VAT number	Value-Added Tax Identification Number.

1.6.2. DEFINITIONS

Activation data	Private data such as PINs or passwords used for activating the private key.
Advanced Electronic Signature	an electronic signature that complies with the requirements specified in Article 26 of the eIDAS Regulation: (a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and

	(d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.
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 Relying 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 CA 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.
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 standardisation and referring to a particular object or object class.
PKI	A set of hardware, software and human resources elements and procedures, etc., that a system is made up of based on the creation and management of public key certificates.
Policy Authority	A person or group of people responsible for all decisions relating to the creation, management, maintenance and removal of certification and CPS policies.
Private key	A mathematical value known only to the Subject/Signatory and used for creating a digital signature or decrypting data. Also called signature creation data. The CA's private key is to be used for signing certificates and CRLs.
Public key	A publicly known mathematical value used for verifying a digital signature or encrypting data. Also called signature verification data.
Qualified electronic signature	Is an electronic signature that is compliant with EU Regulation No 910/2014 (eIDAS Regulation) for electronic transactions within the internal European market. It enables

	to verify the authorship of a declaration in electronic data exchange over long periods of time. Qualified electronic signatures can be considered as a digital equivalent to handwritten signatures.
Qualified Trust Service Provider	A trust service provider that provides one or more qualified trust services and has been recognized as qualified by the Supervisory Body.
Qualified Trust Service	A trust service that complies with the applicable requirements under the eIDAS Regulation.
Registration Authority	The entity responsible for managing applications and identification and registration of certificates. For the purposes of these CPS, the name of "Registration Authority" or "RA" will be applied both in reference to the RAs of Camerfirma.
Relying 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.
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.
Trusted Service	is an electronic service provided by a TSP that may consist of: (a) the creation, verification, validation of electronic signatures or electronic seals or electronic time stamps. It may also be certified electronic delivery services and certificates related to these services; (b) the creation, verification and validation of certificates for the authentication of websites; (c) the preservation of electronic signatures, seals or certificates relating to these services.
Trusted Service Provider	A natural or legal person who provides one or more trust services, either as a qualified provider or as a non-qualified provider of trust services.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. REPOSITORIES

Camerfirma repositories for publication of certification information are available 24 hours a day, 7 days a week.

2.2. PUBLICATION OF CERTIFICATION INFORMATION

2.2.1. CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICIES

Camerfirma makes available to the public its CPS and CPs in https://policy21.camerfirma.com.

2.2.2. TERMS AND CONDITIONS

The Subject, and the Subscriber if they are different persons, receive information on the terms and conditions to be accepted prior to the issuance of the certificate. Relying Parties can also consult Terms and Conditions in Camerfirma website:

- https://www.camerfirma.com/tc/terms_and_conditions21.pdf (English)
- https://www.camerfirma.com/tc/terminos_y_condiciones21.pdf (Spanish)

2.2.3. DISTRIBUTION OF THE CERTIFICATES

Camerfirma makes available to the public its Root CA certificate 'CAMERFIRMA ROOT 2021' in http://ca.camerfirma.com/certs/camerfirmaroot2021.crt.

Camerfirma makes available to the public its Intermediate CA certificate 'AC CAMERFIRMA QUALIFIED CERTIFIATES – 2021' in http://ca.camerfirma.com/certs/camerfirmaqc2021.crt.

It is the responsibility of the Subject to deliver its certificate to anyone requesting to check the validity of its certificate.

2.2.4. REVOCATION LISTS AND OCSP

Revocation lists are published in the certificate public registry, accessible via the HTTP protocol as indicated in the "CRL Distribution Points" of the certificate. Lists can be accessed through compliant products available on the market that can interpret HTTP protocol.

The CAs may provide additional access options to consult the list of published certificates and their validity.

The CAs primary status service for a certificate is the one offered by OCSP.

Camerfirma makes available its OCSP services in: http://ocsp2021.camerfirma.com/

2.3. TIME OR FREQUENCY OF PUBLICATION

A new version of this document will be created at least once a year. Camerfirma immediately publishes on its website any change to this document, maintaining a version document history.

Older versions of documents are kept for a period of at least fifteen (15) years and may be consulted by stakeholders on its website https://policy21.camerfirma.com.

The CAs issues and publishes revocation lists periodically in accordance section 4.9.7.

2.4. ACCESS CONTROLS ON REPOSITORIES

Camerfirma makes its repository available to the public.

Camerfirma uses reliable systems for the repository, so that:

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

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

3. IDENTIFICATION AND AUTHENTICATION

3.1. NAMING

3.1.1. TYPES OF NAMES

The Subject/Signatory is described by a distinguished name (DN, *distinguished name*, Subject) in compliance with the X.500 standard. Certificates are issued according to IETF RFC 5280 specification and ETSI EN 319 412 Parts 2 and 3.

The DN field descriptions are shown in each of the certificate profile sheets. It also includes a *"Common Name"* component (CN =).

See section 7.1 for information about profile records.

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

- Natural persons: In certificates corresponding to natural persons, the identification of the Signatory is made up with their full name and tax ID number.
- The structure for Intermediate CAs, OCSP certificates includes at least:
    - A descriptive name that identifies the CA (CN)
    - The legal entity responsible for the keys (O)
    - The tax ID number of the organization responsible for the keys (*OrganizationIdentifier*)
    - The country where the company responsible for the keys carries out the activity (C)
- The Root CA certificates have a descriptive name that identifies the CA and the (O) field contains the name of the organization responsible from the CA.

3.1.2. NEED FOR NAMES TO BE MEANINGFUL

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

3.1.3. ANONYMITY OR PSEUDONYMITY OF SUBSCRIBERS

Subscribers are not permitted to use pseudonyms.

3.1.4. RULES FOR INTERPRETING VARIOUS NAME FORMS

Camerfirma complies with the ISO/IEC 9594 X.500 standard and IETF RFC 5280.

3.1.5. UNIQUENESS OF NAMES

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

3.1.6. RECOGNITION, AUTHENTICATION, AND ROLE OF TRADEMARKS

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

3.1.7. NAME DISPUTE RESOLUTION PROCEDURE

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

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

3.2. INITIAL IDENTITY VALIDATION

3.2.1. METHOD TO PROVE POSSESSION OF PRIVATE KEY

The keys created by Camerfirma under CPs described in this document:

- In Hardware: The keys can be delivered by Camerfirma to the Subject/Holder/Signatory, directly or through a RA on a qualified signature creation device (QSCD).
- In centralized remote 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-104-2 level 3 or EAL4+ HSM device ensuring the unique control of this key by the Subject/Signer (QSCD).

3.2.2. AUTHENTICATION OF ORGANIZATION IDENTITY

3.2.2.1. IDENTITY

Prior to the issuance and delivery of a certificate issued to a natural person with the attribute of being linked to an entity, it is necessary to authenticate the data relating to the constitution 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 depending on the type of entity. The relevant documentation can be found on the Camerfirma website in the informative section of the corresponding certificate.

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

The Registration Agencies employed for organization identification in Spain are:

- *Registro Mercantil*
- *Agencia Tributaria*
- Specific Registration Agency according Entity type.

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

3.2.2.2. TRADEMARKS

See section 3.1.6.

3.2.2.3. COUNTRY VERIFICATION

See section 3.2.2.1.

3.2.2.4. VALIDATION OF DOMAIN AUTHORIZATION OR CONTROL

No SSL/TLS certificates are being issued by the CAs included in this CPS.

3.2.2.5. AUTHENTICATION OF AN IP ADDRESS

No SSL/TLS certificates are being issued by the CAs included in this CPS.

3.2.2.6. WILDCARD DOMAIN VALIDATION

No SSL/TLS certificates are being issued by the CAs included in this CPS.

3.2.2.7. ACCURACY OF DATA SOURCES

See section 3.2.2.1.

3.2.2.8. CAA

No SSL/TLS certificates are being issued by the CAs included in this CPS and therefore there is no requirement for CAA entries.

3.2.3. AUTHENTICATION OF INDIVIDUAL IDENTITY

Identity Document: Prior to issuance and delivery of a certificate, the verification of Applicant's personal identity is required. The Applicant has to present his/her original Identity Document in force, according to the following requirements:

Spanish nationality:

- *Documento Nacional de Identidad* or Passport.

Foreigners from UE or EEA:

- Passport or Identity Document issued by UE or EEA country and *Certificado de Número de Identidad de Extranjero* (NIE).

Foreigners from other countries residing in Spain:

- Residence Card or Foreigner Identity Card with photography.

Foreigners from other countries no residing in Spain:

- Passport.

For foreign Identity documents, they must be present with Hague Apostille and if deemed necessary with official translation.

Certificates cannot be issued to minors who are not emancipated, who are legally or partially incapacitated, or when there are reasonable suspicions that the Applicant is not in possession of his full mental abilities.

Control over the email address incorporated in the certificate application is verified by communication of a random value that will be required at the time the certificate is generated and downloaded. This check will be carried out exclusively by the CA, so it cannot be delegated.

Identification Methods: the identity of an individual shall be verified using one of the methods indicated in the eIDAS Regulation and in accordance with applicable national law:

1. Physical presence: the physical presence of the Applicant is required in front of a Certification Authority Operator, Registration Authority Operator or an In-person Point of Physical Verification. The Applicant may alternatively choose to come along a Public Notary and provide the certificate issuance request with his/her signature authenticated.
2. Remotely, using electronic identification means, for which prior to the issuance of the qualified certificate, a physical presence of the natural person was ensured and which meets the requirements set out in Article 8 with regard to the assurance levels 'substantial' or 'high' (of eIDAS Regulation). Electronic identification systems notified by Member States under Article 9.1 of the eIDAS Regulation will be accepted. In Spain, the electronic DNI will be accepted.
3. By means of another qualified electronic signature certificate issued by a Camerfirma CA or another Provider, for which the natural person has been identified in person or using electronic identification means in accordance with point 2 above, provided that the natural person's identity data (and, where applicable, the attributes in the certificate requested) are contained in the certificate used.
4. Alternatively, by using other identification methods recognized at national level which provide equivalent assurance in terms of reliability to physical presence, in accordance with the applicable regulation, in particular the conditions and technical requirements established in *Orden ETD/465/2021*, of May 6, of the Spanish *Ministerio de Asuntos Económicos y Transformación Digital* which regulates remote video identification methods for the issuance of qualified electronic certificates. The identification of the Applicant may be carried out in an assisted way, with the synchronous mediation of an operator, or in an unassisted way, without online interaction between an operator and the Applicant, but with a subsequent revision by an operator.

   Camerfirma makes available to its users, various remote identification processes by video, which may be used to issue qualified electronic certificates, as long as they comply with the conditions and technical requirements required by the applicable regulation, which must be confirm in a Conformity Assessment Report issued by a Conformity Assessment Body, specifically the following:

   - Assisted process with synchronous mediation of an operator.
   - Assisted process with pre-validation of documentation and synchronous mediation of an operator.
   - Unattended process without online interaction with an operator, but with subsequent revision by an operator.

In all processes, the following additional measures shall be applied:

- If the Applicant has submitted a DNI or NIE, Camerfirma must consult the Applicant's identity data through the intermediation platform of the Data Verification and Consultation Service that the Supervisory Body makes available, provided that the technical requirements of the platform and the DNI or NIE accreditation support allow it.
- Registration data, i.e. audio and video files and structured metadata in electronic format, are stored in a protected manner and in accordance with the European standard on personal data protection.

- For security and fraud prevention purposes, only conventional identity documents will be accepted under this method of identification (Spanish ID cards and Spanish or foreign passports). The identification of foreign Applicants who do not have a Passport, may be authorised by the CA after reviewing the objective characteristics of their identity documents in terms of certainty of identification, security of the CA and specific training.

The provisions of this section on the obligation to verify the identity and other circumstances of the Applicants for a qualified certificate may not be required when the identity or other permanent attributes of the certificate Applicants are already known by Camerfirma or the RA by virtue of a pre-existing relationship, in which, for the identification of the interested party, the means indicated in point 1 were used and the period of time that has elapsed since the identification is less than five years.

3.2.4. NON-VERIFIED SUBSCRIBER INFORMATION

It's not allowed to include non-verified information in the "Subject" of a certificate.

3.2.5. VALIDATION OF AUTHORITY

3.2.5.1. PROOF OF RELATIONSHIP

Certificate type	Documentation
QUALIFIED CERTIFICATE FOR A LEGAL REPRESENTATIVE OF A LEGAL ENTITY – QCP-n-qscd QUALIFIED CERTIFICATE FOR A LEGAL REPRESENTATIVE OF A NON-LEGAL ENTITY – QCP-n-qscd QUALIFIED CERTIFICATE FOR A VOLUNTARY REPRESENTATIVE OF A LEGAL ENTITY BEFORE THE PUBLIC ADMINISTRATIONS – QCP-n-qscd QUALIFIED CERTIFICATE FOR A VOLUNTARY REPRESENTATIVE OF A NON-LEGAL ENTITY BEFORE THE PUBLIC ADMINISTRATIONS – QCP-n-qscd QUALIFIED CERTIFICATE FOR A SPECIAL REPRESENTATIVE OF A LEGAL ENTITY – QCP-n-qscd QUALIFIED CERTIFICATE FOR A SPECIAL REPRESENTATIVE OF A NON-LEGAL ENTITY – QCP-n-qscd	Evidence on the Subject/Signatory's representation powers with respect to the entity, by providing documentation showing their powers of attorneys depending on the type of entity. This information is published in the RA's operating manuals and in Camerfirma's website.
QUALIFIED CORPORATE CERTIFICATE – QCP-n-qscd	Usually, an authorisation signed by the entity's Legal Representative.

According to article 24.2.h) of the eIDAS Regulation, this registration activity may be carried out by electronic means, both if the documents provided are valid electronic documents as well as paper documents. In the latter case, the Registry Operator must keep a scanned copy and digitally sign it with its Digital Certificate, for preservation in computer files.

3.2.5.2. SERVICE OR MACHINE IDENTITY

No SSL/TLS certificates are being issued by the CAs included in this CPS.

3.2.5.3. USER IDENTIFICATION CONSIDERATIONS FOR SENIOR MANAGEMENT ROLES

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

3.2.5.4. SPECIAL CONSIDERATIONS FOR ISSUING CERTIFICATES OUTSIDE OF SPANISH TERRITORY

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

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

The re-key requests of a certificate is the process that must be carried out to obtain a new key pair and a new certificate when its expiration date is close, the certificate has expired or has been revoked.

3.3.1. IDENTIFICATION AND AUTHENTICATION FOR ROUTINE RE-KEY

The identification of a re-key application can be made using the same methods as for the initial identity validation (section 3.2), including the use of the certificate to be re-keyed, or if the Applicant's identity or other permanent circumstances and the identification of the interested party have been carried out in person for less than five years.

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 re-key takes place on end 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 a physical presence, if usually required due to the nature of the certificate, is not necessary if the certificate was issued less than five years ago.

3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

The method for submitting revocation requests is established in section 4.8 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

4.1. CERTIFICATE APPLICATION

4.1.1. WHO CAN SUBMIT A CERTIFICATE APPLICATION

Applications for qualified certificates for natural persons must be submitted by the Applicant (see section 1.3.5.4):

4.1.2. ENROLLMENT PROCESS AND RESPONSIBILITIES

The registration process includes Applicant application, identification, delivery of additional documentation related to the entity and representative status (could be uploaded), generation of the key pair, public key certification request, and signature of the contract (not necessarily in that order).

Each party involved in the process has specific responsibilities and jointly contributes to successful certificate issuance:

- The Applicant/Subject is responsible for providing correct and truthful information on his identity and on specific attributes of the Subject, reading carefully the material made available by the CA – including through the RA – and following CA and/or RA instructions while submitting a qualified certificate application. If the Subject is a legal person, those responsibilities fall on the legal representative or the attorney who submits the qualified certificate application;

- The Subscriber, if present, is responsible for informing the Subject on whose behalf he is requesting a certificate about the obligations arising from the certificate, as well as for providing correct and truthful information about the identity of the Subject and for following processes and indications given by the CA and/or RA;
- The RA, if present, is responsible for – including through the Registration Operator – the Subject identification or the Subscriber identification if the Subject is a legal person, and for the accuracy and validity of the attributes of the Subject (in case of certificate with attributes), informing them about the obligations derived from the certificate and following in detail the processes defined by the CA;
- The CA is ultimately responsible for Subject/Subscriber identification, verification of attributes and successful registration of the qualified certificate.

4.2. PROCESSING THE CERTIFICATION REQUEST

To obtain a signature certificate, the Subject and/or Subscriber must:

- Carefully read this CPS, the Terms and Conditions and any additional information material;
- Comply with the identification procedures adopted by the CA as described in section 3.2.3;
- Provide all information required for identification together with any appropriate documentation (when required);
- Provide all information required for attributes existence and validity with any appropriate documentation (when required)
- Sign the registration and certification request and accept the contractual terms governing service provision, using the relevant analogical or electronic forms established by the CA.

The information to be provided by the Subject:

- Natural person. In case of a certificate requested for a natural person the following information must be provided by the Subject and/or Subscriber:
    - Surname and Name
    - Date and Place of Birth;
    - Tax Code or similar identification code (TIN).
    - Residence address;
    - References of the ID proof used for identification (e.g. document type, number, issuer and date of issue);
    - An email address for submission of communications from the CA to the Subject;
    - A mobile phone number for OTP delivery, where this OTP technology is used.

  The email address and mobile phone number provided to the RA, shall be valid and shall uniquely identify the Subject. The email address shall be used for any communications from the RA and for sending emergency codes (ERCs) and expiry notices.

- Legal person. In case of a certificate requested for a legal person the following information must be provided by the Subscriber that acts as legal representative or attorney of the legal person:
    - Surname and Name of the Subscriber;
    - Tax Code or similar identification code (TIN) held by the Subscriber;
    - References of the document ID used for Subscriber identification (e.g. document type, number, issuer and date of issue);
    - An email address for transmission of communications from the CA to the Subscriber;
    - Name of the Subject (legal person);
    - VAT Number.

- Specific attributes. In case of certificate requested for a natural person with specific attributes related to his/her business relationship with an entity:
    - Charge or post in the entity (optional)
    - Department 1
    - Department 2 (optional)

- Specific attributes. In case of certificate requested for a natural person with specific attributes related to his/her representative / powers of attorney status with an entity:
    - Charge or post in the entity (optional)
    - Department 1

- Department 2 (optional)
- Public deed / Powers of attorney references

The information provided is stored in the CA archives (registration phase) and serves as a basis for generating the qualified certificate.

4.2.1. PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS

During the initial registration and collection of registration and certification applications phase, the Subject or the Subscriber acting as legal representative of a legal person receives a security code that enables him/her to activate the signature device or signature process if it is remote. Security codes are delivered in a security envelope or, if electronic, are transmitted in encrypted files.

The CA may provide that the signature PIN is independently selected by the Subject or Subscriber who is legally representing a legal person. In such cases, is the responsibility of the Subject/Subscriber to remember the PIN.

The CA can also provide that the remote procedure signature certificate can be used through an authentication system provided by the RA, having at least significant security level, or provided, after analyzing the characteristics of the system itself, within the scope of certification of the secure signature device. In these cases, the authentication system can also be used for any request for revocation of the certificate.

4.2.2. APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS

Following initial registration, the CA or RA may refuse to complete the issuance of a signature certificate due to lack of or incomplete information, consistency and anti-fraud checks, where the identity of the Subject/Subscriber is unclear etc.

4.2.3. TIME TO PROCESS CERTIFICATE APPLICATIONS

The time lag between registration application and certificate issuance depends on the application method chosen by the Subject, or by the Subscriber, and on whether any additional information needs to be collected or the device is to be physically delivered.

4.2.4. NOTIFICATION TO SUBSCRIBER BY THE CA OF ISSUANCE OF CERTIFICATE

In the end entity certificates issued by Camerfirma a notification is sent by email to the Applicant indicating the approval or denial of the request.

4.3. CERTIFICATE ISSUANCE

4.3.1. CA ACTIONS DURING CERTIFICATE ISSUANCE

4.3.1.1. CERTIFICATES ISSUED ON A CRYPTOGRAPHIC SMARTCARD OR TOKEN

The RA generates the cryptographic key pair directly on a secure signature device using the applications supplied to it by the CA after secure authentication.

The RA sends the CA a public key certification request in PKCS#10 format. The request is digitally signed with a specially authorised, qualified signature certificate. After confirming that the signature on the PKCS#10 is authentic and that the subject is entitled to submit the request, the CA generates a qualified certificate that is sent through a secure channel located inside the device.

4.3.1.2. CERTIFICATES ISSUED ON A REMOTE SIGNATURE DEVICE (HSM)

The Subject or the Subscriber log on to the RA services or applications.

The RA generates the cryptographic key pair directly on the HSM located at the QTSP premises. Then the RA sends to the CA a public key certification request through a secure channel.

After confirming that the subject is entitled to submit the request, the CA generates a qualified certificate that is stored in the HSM.

The qualified devices fulfill the policy of the signature creation application service component: itu-t(0) identified-organization(4) etsi(0) SERVICE CREATION-policies(19431) ades(2) policy-identifiers(1) eu-advancedx509(2) – [0.4.0.19431.2.1.2].

4.3.1.3. CERTIFICATES ISSUED FOR TESTING PURPOSES

Sometimes it is necessary to use certificates to perform some tests in a production environment.

In these cases, before issuing the certificate it is necessary to proceed with the registration of the data. This registration must be approved by the Security Officer.

The data used for registration must clearly indicate in the Subject that it is a test certificate and not an actual certificate.

This procedure cannot be used for load tests or cyclic tests on registrations and emissions. When the specific test session is no longer needed, the certificate must be revoked ex officio.

4.3.2. NOTIFICATION TO SUBSCRIBER BY THE CA OF ISSUANCE OF CERTIFICATE

If the certificate is issued on a cryptographic device, the Subject or the Subscriber does not need to be notified of the certificate issuance as the certificate is stored in the device delivered to him.

In other cases, the Subject will receive the notification via the email address indicated at the time of registration. This information can also be shared with the Subscriber.

4.3.3. ACTIVATION

4.3.3.1. ACTIVATION OF THE SIGNATURE DEVICE (SMARTCARD OR TOKEN)

After receiving the device, the Subject, using the activation codes confidentially given to him and the special software provided by the CA, proceeds to activate the device choosing at the same time a signature PIN, a confidential security parameter whose secrecy and protection are placed exclusively on the Subject itself.

4.3.3.2. ACTIVATION OF REMOTE SIGNATURE DEVICE (HSM)

After logging on to the CA website using the activation codes confidentially given to him, the Subject – or, in case of a legal person, the Subscriber – selects a signature PIN, a confidential security parameter whose secrecy and protection are placed exclusively on the Subject itself. To confirm the PIN, the Subject/Subscriber enters the One Time Password received via SMS, generated via token or the token-app associated with the certificate.

In some cases, the certificate can be issued already active and usable.

4.4. CERTIFICATE ACCEPTANCE

4.4.1. CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE

Once the certificate has been delivered or notified, the user has fourteen 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

Following successful completion of the certification procedure, the certificate will be entered in the relevant Certificate Registry and will not be made public by the CA.

4.4.3. NOTIFICATION OF THE ISSUANCE TO THIRD PARTIES

Not stipulated.

4.5. KEY PAIR AND CERTIFICATE USAGE

4.5.1. SUBSCRIBER PRIVATE KEY AND CERTIFICATE USAGE

Any signature device or remote signature authentication tool must be kept by the Subject in a secure manner. The Subject must keep private key usage validation information separately from the device, if present, or from the tools or authentication codes. He must further ensure the protection of privacy and the preservation of the emergency code required for certificate revocation, while using his certificate solely in the manner prescribed by this CPS and by applicable national and international laws.

The Subscriber must not place any electronic signatures using private keys for which the relevant certificate has been revoked and must refrain from using signature certificates issued by revoked CAs.

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

CA	Key Usage	Extended Key Usage	Basic Constraints
CAMERFIRMA ROOT 2021	critical, cRLSign, keyCertSign	-	critical,CA:true
AC CAMERFIRMA QUALIFIED CERTIFICATES – 2021	critical, cRLSign, keyCertSign	emailProtection clientAuth	critical,CA:true
QUALIFIED CORPORATE CERTIFICATE – QCP-n-qscd in QSCD SmartCard or Token	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
QUALIFIED CORPORATE CERTIFICATE – QCP-n-qscd in QSCD Cloud	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
QUALIFIED CERTIFICATE FOR A LEGAL REPRESENTATIVE OF A LEGAL ENTITY – QCP-n-qscd in QSCD SmartCard or Token	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
QUALIFIED CERTIFICATE FOR A LEGAL REPRESENTATIVE OF A LEGAL ENTITY – QCP-n-qscd in QSCD Cloud	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
QUALIFIED CERTIFICATE FOR A LEGAL REPRESENTATIVE OF A NON-LEGAL ENTITY – QCP-n-qscd in QSCD SmartCard or Token	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
QUALIFIED CERTIFICATE FOR A LEGAL REPRESENTATIVE OF A NON-LEGAL ENTITY – QCP-n-qscd in QSCD Cloud	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
QUALIFIED CERTIFICATE FOR A VOLUNTARY REPRESENTATIVE OF A LEGAL ENTITY BEFORE THE PUBLIC ADMINISTRATIONS – QCP-n-qscd in QSCD SmartCard or Token	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
QUALIFIED CERTIFICATE FOR A VOLUNTARY REPRESENTATIVE OF A LEGAL ENTITY BEFORE THE PUBLIC ADMINISTRATIONS – QCP-n-qscd in QSCD Cloud	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
QUALIFIED CERTIFICATE FOR A VOLUNTARY REPRESENTATIVE OF A NON-LEGAL ENTITY BEFORE THE PUBLIC ADMINISTRATIONS – QCP-n-qscd in QSCD SmartCard or Token	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
QUALIFIED CERTIFICATE FOR A VOLUNTARY REPRESENTATIVE OF A NON-LEGAL ENTITY BEFORE THE PUBLIC ADMINISTRATIONS – QCP-n-qscd in QSCD Cloud	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
QUALIFIED CERTIFICATE FOR A SPECIAL REPRESENTATIVE OF A LEGAL ENTITY – QCP-n-qscd in QSCD SmartCard or Token	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
QUALIFIED CERTIFICATE FOR A SPECIAL REPRESENTATIVE OF A LEGAL ENTITY – QCP-n-qscd in QSCD Cloud	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
QUALIFIED CERTIFICATE FOR A SPECIAL REPRESENTATIVE OF A NON-LEGAL ENTITY – QCP-n-qscd in QSCD SmartCard or Token	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false

CA	Key Usage	Extended Key Usage	Basic Constraints
QUALIFIED CERTIFICATE FOR A SPECIAL REPRESENTATIVE OF A NON-LEGAL ENTITY – QCP-n-qscd in QSCD Cloud	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false

Although data encryption with certificates is technically possible, Camerfirma is not responsible for any resulting damages should the holder not be able to retrieve the private key required to decipher the information.

4.5.2. RELYING PARTY PUBLIC KEY AND CERTIFICATE USAGE

Relying Parties must be familiar with the certificate's scope of use as indicated in the CPS and in the certificate itself. They must also confirm a certificate's validity before using the public key contained in it, ensure that the certificate has not been revoked by checking the relevant OCSP service or CRL and confirm the existence and content of any key pair use restrictions, as well as of any representation powers and professional qualifications.

4.6. CERTIFICATE RENEWAL

N/A

4.7. CERTIFICATE RE-KEY

4.7.1. CIRCUMSTANCE FOR CERTIFICATE RE-KEY

Certificate re-key involves issuance of a new key pair and a signature certificate used to sign documents and transactions.

Root CA and Intermediate CAs 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.

4.7.2. WHO MAY REQUEST CERTIFICATE RE-KEY

The Subject may request re-key a certificate prior to its expiration only if the certificate has not been revoked and if all the information provided upon previous issuance is still applicable. A certificate may not be re-keyed after its expiration date, and a new certificate should be requested instead.

4.7.3. PROCESSING CERTIFICATE RE-KEY REQUESTS

Certificate re-key is performed through a specific service provided by the CA as part of its business and contractual relations with the Subject and with the RA.

4.7.4. NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

The notification of the issuance of a re-keyed certificate it will occur as stipulated in section 4.3.2 of this document.

4.7.5. CONDUCT CONSTITUTING ACCEPTANCE OF A RE-KEYED CERTIFICATE

As stipulated in section 4.4.1 of this document.

4.7.6. PUBLICATION OF THE RE-KEYED CERTIFICATE BY THE CA

As stipulated in section 4.4.2 of this document.

4.7.7. NOTIFICATION OF THE RE-KEYED CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

In some cases, end entity certificates are sent to the Supervisory Body that regulate the activities of the CAs.

OCSP certificates are communicated to different government agencies that have a certificate validation platform.

The Root CA and Intermediate CAs certificates are notified to the Supervisory Body for incorporation into the TSL.

4.8. CERTIFICATE MODIFICATION

N/A

4.9. CERTIFICATE REVOCATION AND SUSPENSION

If a certificate is revoked, it is invalidated before its expiration date. Any signatures placed after the revocation is published become invalid. Revoked certificates are marked as such in the OCSP service and in the CRL signed by the CA. This list is issued and published at set intervals, see Section 4.9.7. Under special circumstances, the CA may force issuance of an unplanned CRL. Revocation become effective as of the time of issuance of the list, which is certified by the date of event registration entered in the CA's Audit Log.

The revocation status information is kept available at a CA (Root or Intermediate) for 15 years after the expiry of the Root CA certificate by issuing and storing the last CRL.

Certificate suspension is not allowed.

Camerfirma maintains the information about the status of an expired certificate through the OCSP and/or CRL services.

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

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

Revoked certificates cannot be used under this CPS.

4.9.1. CIRCUMSTANCES FOR REVOCATION

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.
- Termination of the CA.

Due to circumstances affecting key or certificate security:

- The private key or infrastructures or systems belonging to the CA that issued the certificate are compromised, whenever this incident affects the accuracy of the issued certificates.
- The CA has breached the requirements in the certificate management procedures established in this CPS.
- The security of the key or certificate belonging to the Subject or the Responsible for the certificate is compromised or suspected of being compromised.
- There is unauthorized third party access or use of the private key of the Subject or the Responsible for the certificate.
- There is misuse of the certificate by the Subject or the 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 unauthorized third-party access to the activation details of the Subject/Signatory or the responsible for the certificate.
- Non-compliance by the Subscriber, the Subject or the Responsible of the rules of use of the cryptographic device set forth in this CPS or in Terms and Conditions.

There are circumstances that affect the Subject, Subscriber, the Entity or the Responsible for the certificate:

- The relationship is terminated between the CA and the Subscriber.
- There are changes to or termination of the underlying legal relationship or cause for issuing the certificate to the Subject.
- The Applicant breaches part of the requirements established for requesting the certificate.
- The Subject, Entity or the Responsible for the certificate breach part of their obligations, responsibility and guarantees established in the Terms and Conditions in this CPS.

- The sudden incapacity or death of the Subject.
- There is a termination of the entity related to the Subject/Signatory of the certificate.
- The authorisation provided by the Subscriber to the Subject or to the Responsible for the certificate has changed or expired, or the relationship between the Subject and the Responsible for the certificate has finished.
- The Subject requests revocation of the certificate in accordance with the provisions of this CPS.
- Firm resolution of the competent administrative or judicial authority.
- The Subject indicates that the original certificate request was not authorized and does not grant the authorization retroactively.
- In case the Applicant, the Subject or the Responsible request the CA to modify or delate his/her personal data from Camerfirma registers.

Other circumstances:

- For the issuance of a certificate that does not meet the requirements set forth in this CPS.
- Termination of the CA's service, in accordance with the corresponding section of this CPS except if the management of the issued certificates has been transferred to another Provider.

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 revocation is requested by the Subject or the Subscriber, 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 Subject or the legal representative of the 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 Subject due to termination of the relationship with it, this circumstance must be evidenced (revocation of Powers of Attorney, contract termination, etc.) and the Applicant must identify him/herself to the RA as authorised to represent the entity.

4.9.2. WHO CAN REQUEST REVOCATION

The request of the certificate revocation can be done by:

- The Subscriber.
- The Subject/Holder.
- The Responsible.
- The Entity. Via a representative, when the Subject is a natural person associated with an organization.
- The RA or CA.
- It also contemplates the possibility that third parties or interested parties can communicate frauds, misuses, inappropriate behavior, or erroneous data, in which case, the RA or the CA may revoke the certificate after verifying the veracity of said causes of revocation.

The request for revocation of the certificate can be managed by:

- The authorized operators of the CA or the RA (Responsible for Revocation).

Additionally, the authorized operators of the CA may process the request for massive revocation of certificates due to the cessation of activity of the CA or an RA.

In any case, at the time the certificate is revoked, an email notification will be sent to the Subject (electronic signature certificate) specifying the date and time and the reason for the revocation.

4.9.3. PROCEDURE FOR REVOCATION REQUEST

A revocation can be requested by entitled subjects using the following procedures.

4.9.3.1. REVOCATION REQUEST BY THE SUBJECT OR BY THE RESPONSIBLE

The revocation request is submitted by the Subject or by the Responsible using the forms available on the CA website. The request must be signed by the revocation requester and delivered to the RA or, alternatively, sent to the CA by letter, fax or email accompanied by a copy of a valid ID document. Furthermore, the CA or RA can make available additional

methods for submitting the request for revocation, as long as those methods provide for a correct identification of the Subject.

Upon confirmation of the authenticity of the request, the CA revokes the certificate and promptly notifies the Subject of the revocation.

If attribute information is included in the certificate referred to in the revocation request, the revocation will be notified by the CA to the Subscriber with whom the CA has entered into special agreements. If the name of the Entity is included in the certificate referred to in the revocation request, the CA shall notify such Entity.

Additional methods for requesting revocation by the Subject may be specified in any agreements between the Subject and the CA.

4.9.3.2. REVOCATION REQUEST BY THE ENTITY OR THE SUBSCRIBER

The same methods applicable for revocation request by the Subject or by the Responsible apply for the revocation request of the Subject's certificate submitted by the Entity or the Subscriber. The Entity, via a representative, shall specify the Subject details as provided to the CA at the time of certificate issuance.

Upon confirmation of the authenticity of the request, the CA notifies the Subscriber and Subject by the communication means established upon certificate request and revokes the certificate. Additional methods for revocation requests may be specified in any agreement between the Subject and the CA or RA.

4.9.3.3. REVOCATION BY THE CA/RA EX OFFICIO

Where necessary, the CA/RA may revoke a certificate by giving prior notice to the Subject and specifying the circumstances for revocation as well as the date and time of effect.

If attribute information is included in the certificate to be revoked, the revocation will be notified by the CA/RA to the Subscriber with whom the CA has entered into special agreements. If the name of the Entity is included in the certificate referred to in the revocation request, the CA shall notify the revocation to such Entity. The CA/RA will communicate the revocation also to the Subscriber.

4.9.4. REVOCATION REQUEST GRACE PERIOD

Camerfirma may grant revocation grace periods on a case-by-case basis.

4.9.5. TIME WITHIN WHICH CA MUST PROCESS THE REVOCATION REQUEST

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

The maximum time from receipt of a revocation request to its confirmation and processing shall be 23 hours. If the revocation request cannot be confirmed within this time, it will not be processed.

The CA shall immediately process revocation requests that are confirmed and processed. The maximum time from processing to publication in the state information services is 1 hour.

The revocation status will be published no later than 24 hours after receipt of the revocation request, in accordance with current regulations.

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 this CPS, 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

Relying parties must check the status of the certificates either by consulting the CRLs or the OCSP services.

4.9.7. CRL ISSUANCE FREQUENCY

The CRL of the Root CA 'CAMERFIRMA ROOT 2021' has a maximum issuance frequency of 365 days. May be issued within the next hour after a certificate issued by this Root CA is revoked.

The CRL of the Intermediate CA 'AC CAMERFIRMA QUALIFIED CERTIFICATES – 2021' has an issuance frequency of 1 hour.

4.9.8. MAXIMUM LATENCY FOR CRLS

The CRL of the Root CA 'CAMERFIRMA ROOT 2021' is published within the next 23 hours after its issuance, before the end of validity of the previous CRL.

The CRL of the Intermediate CA 'AC CAMERFIRMA QUALIFIED CERTIFICATES – 2021' is published when it is issued, before the end of validity of the previous CRL.

4.9.9. ON-LINE REVOCATION/STATUS CHECKING AVAILABILITY

All CAs described in this CPS provide an OCSP certificate status checking service, until the Root CA of the hierarchy certificate expires or until the CA has issued a last CRL after performing a mass revocation of all the active certificates.

4.9.10. ON-LINE REVOCATION CHECKING REQUIREMENTS

To check the online revocation of a certificate by the OCSP service:

- Camerfirma shall make the OCSP services available to the relying parties with the possibility of using GET and POST methods.
- Camerfirma shall update the information provided via the OCSP service of the Root CA 'CAMERFIRMA ROOT 2021' within the next 24 hours after a certificate issued by this Root CA is revoked.
- Camerfirma shall update the information provided via the OCSP service of the Intermediate CA 'AC CAMERFIRMA QUALIFIED CERTIFICATES – 2021' OCSP service in real time.

4.9.11. OTHER METHODS OF DISCLOSING REVOCATION INFORMATION

N/A

4.9.12. SPECIAL REVOCATION REQUIREMENTS DUE TO COMPROMISED KEY SECURITY

Parties that detect a key compromise may notify it by sending an email to the email address incidentes@camerfirma.com with the subject "*Key compromise notification*" including the private key that has been compromised.

4.9.13. CIRCUMSTANCES FOR SUSPENSION

The CAs in this CPS do not suspend certificates.

4.9.14. WHO CAN REQUEST SUSPENSION

Not applicable.

4.9.15. PROCEDURE FOR SUSPENSION REQUEST

Not applicable.

4.9.16. LIMITS ON SUSPENSION PERIOD

Not applicable.

4.10. CERTIFICATE STATUS SERVICES

4.10.1. OPERATIONAL CHARACTERISTICS

Certificate status information is available through CRLs and OCSP services.

Camerfirma shall make the CRLs publicly available in the URLs that are included in the extension CRL Distribution Points of each certificate.

CRLs issued by the Intermediate CA 'AC CAMERFIRMA QUALIFIED CERTIFICATES – 2021' include expired certificates.

Revoked certificates that have expired when the Root CA 'CAMERFIRMA ROOT 2021' issues the CRL will not appear in it. In the event this Root CA termination, Camerfirma shall include each revoked certificate, even expired certificates, its revocation reason and revocation time in the last CRL.

Camerfirma shall include the access URL to the OCSP services in the extension called Authority Information Access in each certificate in the certification chain, except in the Root CA certificates.

Camerfirma shall provide information on the status of expired certificates via OCSP services after their expiry date.

4.10.2. SERVICE AVAILABILITY

Certificate status services are available 24 hours a day, seven days a week.

In case of any factor which is not under the control of the CAs, efforts will be made to ensure that this information service are available in 24 hours or less.

4.10.3. OPTIONAL FEATURES

Not stipulated.

4.11. END OF SUBSCRIPTION

The relationship between the Subject and/or Subscriber with the CAs is terminated when the certificate expires or is revoked, except in special cases defined by contract.

4.12. KEY ESCROW AND RECOVERY

Not stipulated.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

Camerfirma as a TSP has implemented an information security system for its digital certification service. The security system is divided into three levels:

- A physical level aimed at ensuring the security of environments where TSP manages the service;
- A procedural level of strictly organizational nature;
- A logical level involving provision of hardware and software technology to address the problems and risks associated with the type of service and the infrastructure used.

This security system is designed to avoid the risks arising from the malfunction of systems, networks and applications, as well as unauthorized interception or data modification.

An excerpt of the Camerfirma security policy can be requested at https://www.camerfirma.com/contacto-soporte/ or by telephone +34 91 344 37 43.

5.1. PHYSICAL SECURITY CONTROLS

The implemented measures provide adequate security on:

- Site and construction features;
- Active and passive anti-intrusion systems;
- Physical access control;
- Power supply and air conditioning;
- Fire protection;
- Flood protection;
- Magnetic media storage modes;
- Magnetic media storage sites.

5.1.1. SITE LOCATION AND CONSTRUCTION

Camerfirma uses three facilities:

- The first one is owned by Camerfirma and stores the CA keys of the Root CA 'CAMERFIRMA ROOT 2021' used for signing certificates and CRLs and the required actions related to them are performed there.
- Camerfirma also use the facilities of its parent company InfoCert. In these facilities the keys of the intermediate CA 'AC CAMERFIRMA QUALIFIED CERTIFICATES – 2021' used for signing certificates and CRLs are stored, and the required actions related to them are performed there.
- Camerfirma uses AWS cloud for the OCSP services for the full hierarchy.

These facilities are located in:

- Camerfirma's facilities are located in Ávila, Spain. It's 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.
- InfoCert Data Center is located in Padova, Italy. The Disaster Recovery site is in Modena and is connected to the above Data Center by a dedicated redundant connection on two separate MPLS 40 Gbit/s each circuit upgradable to 100 Gbit/s.
  Within both sites, rooms protected with several physical and logical security systems have been created. Each room hosts the computer equipment that is at the core of the digital certification, time stamping and remote/automatic signature services.
- For services that need business continuity with RTO/RPO values close to zero, some components of the CAs services relating to publication of the CRLs and the OCSP are hosted on AWS cloud, respectively, in Frankfurt Europe Region and in Ireland Europe Region.
  AWS has certifications of conformity in accordance with the ISO/IEC 27001:2013, 27017:2015, 27018:2019 and ISO/IEC 9001:2015 standards.

5.1.2. PHYSICAL ACCESS

Access to the Camerfirma, InfoCert and AWS Data Centers are governed by the Camerfirma, InfoCert and AWS security procedures.

5.1.3. POWER AND AIR CONDITIONING

Camerfirma Data Center has voltage stabilizers and dual power supply system with one generator.

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

While not certified as such, the site hosting InfoCert Data Center in Padova meets the requirements of a Tier 3 Data Center.

The technical rooms are equipped with an electric power supply system designed to prevent failures, especially malfunctions. Power systems feature state-of-the-art technology to increase reliability and ensure redundancy of the more critical features required by the delivered services.

The power supply infrastructure includes:

- Uninterruptible power supply units, with accumulators and based on alternating current (UPS);
- Alternating Voltage availability (220-380V AC);
- Cabinets powered by redundancy with protected lines sized for the agreed absorption;
- Emergency generator service;
- Automatic switching and synchronisation between generators, network and batteries (STS).

Each technology cabinet installed at the Data Center is powered by two power lines that assure the HA in case of outage of one of the two available lines.

The technology cabinet is monitored remotely, with constant power line status (on/off) and power consumption checks (each line must not exceed 50% of the load).

Temperature inside the technical area is normally kept between 20° and 27°, with relative humidity level of 30% to 60%. Systems are equipped with condensing batteries with a sealed collection and drainage system of the condensate controlled by anti-flooding probes. The entire conditioning system is dedicated to emergency generators in case of power failure. Cooling capacity for each cabinet is ensured with a maximum expected load of 10KW and a maximum of 15KW on two flanked cabinets.

5.1.4. WATER EXPOSURES

Camerfirma Data Center is in an area with a low flooding risk and are not on the ground floor. The rooms in which computer equipment is stored have a humidity detection system.

The location of the site does not pose risks to the environment resulting from proximity to dangerous installations. During building design, appropriate arrangements have been made to isolate potentially hazardous premises, such as those containing the generator set and the thermal plant. Equipment room is on the ground floor above street level.

5.1.5. FIRE PREVENTION AND PROTECTION

Camerfirma Data Center includes an automatic fire detection and extinguishing systems. Cryptographic devices and supports that store CA keys have a specific and additional fire protection system relative to the rest of the facility.

InfoCert Data Center hosts a smoke detection system operated by a NOTIFIER-addressable analogue station with optical sensors positioned in the environment and in the false ceiling and air sampling sensors installed underfloor and in air ducts.

The automatic fire detection system is connected to eco-friendly gas suppression systems NAFS125 and PF23 and, in some rooms, to aerosol shut-off systems. In the event of simultaneous activation of two detectors in the same area, the gas is discharged into the area concerned.

Each fire compartment has a dedicated fire extinguishing system.

In addition, portable extinguishing media compliant with applicable laws and regulations are present.

Primary air ducts attached to equipment rooms are equipped with fire extinguishing shutters at the crossing of fire compartments. These shutters are operated by the automatic fire detection system.

5.1.6. MEDIA STORAGE

Each demountable storage device 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 authorisation.

With regard to the storage platform, the current solution uses NetApp systems (FAS 8060) for the NAS part. For the SAN part an infrastructure for the call center based on Infinidat technology was implemented, including no. 2 enclosure InfiniBox of generation F4000 and F6000; for the CA part, the infrastructure is based on Pure Storage technology.

5.1.7. WASTE DISPOSAL

Camerfirma and InfoCert are ISO 14001 certified for sustainable environmental management of its production cycle, including differentiated waste collection and sustainable waste disposal. Regarding the information content of electronic waste, all media are cleansed of data prior to disposal according to applicable procedures or through certified sanitation companies.

5.1.8. OFF-SITE BACKUP

Camerfirma keeps documents, magnetic and electronic devices safe, which is separate from the operating center in a secure external building. At least two expressly authorised people are required to access, store or withdraw devices.

InfoCert off-site backup takes place at the Disaster Recovery site through an *EMC Data Domain 4200* device, on which the primary *Data Domain* of the Padova site replicates backup data.

5.2. PROCEDURAL CONTROLS

5.2.1. TRUSTED ROLES

Key roles are covered by personnel having the necessary experience, professionalism and technical/legal expertise, which are constantly verified through annual assessments.

Camerfirma trusted roles guarantees the distribution of duties to share out control and limit internal fraud and prevent one person from controlling the entire certification process from start to finish, and with minimum privilege granted wherever possible.

To determine the sensitivity of the function, the following items are considered:

- Duties associated with the role.

- Access level.
- Monitoring operation.
- Training and awareness.
- Required skills.

Camerfirma trusted roles are in accordance with ETSI EN 319 401 and ETSI EN 319 411-1:

- Security Officers: Overall responsibility for administering the implementation of the security practices.
- System Administrators: Authorized to install, configure and maintain the TSP's trustworthy systems for service management and, if required, recovery of the system.
- System Operators: Responsible for operating the TSP's trustworthy systems on a day-to-day basis. Authorized to perform system backup.
- System Auditors: Authorized to view archives and audit logs of the TSP's trustworthy systems.
- Registration Officers: Authorized to perform natural and legal person identification and authorized certificates issuance.
- Revocation Officers: Authorized to perform natural and legal certificates revocation.

5.2.2. NUMBER OF PERSONS REQUIRED PER TASK

Camerfirma and InfoCert guarantees that at least two people will carry out tasks classified as sensitive, mainly those related to the keys of the CAs.

5.2.3. IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE

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 login/password, digital certificates, or physical keys, or SmartCard or Token and activation codes.

5.2.4. ROLES REQUIRING SEPARATION OF DUTIES

The Security Officer trusted role cannot be performed by the same individuals who perform any other trusted role.

5.3. PERSONNEL CONTROLS

5.3.1. QUALIFICATIONS, EXPERIENCE, AND CLEARANCE REQUIREMENTS

Camerfirma personnel who carry out tasks classified as trustworthy must have at least one year's seniority at the work center and a permanent employment contract.

Camerfirma 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 Operators are trustworthy and belong to a Chamber of Commerce or the body delegated to undertake registration work.

RA Operators 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 misdemeanor 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.

Camerfirma, following the annual Human Resource planning, the Function/Organizational Structure Manager identifies the characteristics and skills of the resource to be hired (job profile). Subsequently, in conjunction with the Staff Selection Manager, the search and selection process begins.

5.3.2. BACKGROUND CHECK PROCEDURES

Camerfirma Human Resource 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.

Camerfirma selected candidates participate in the selection process by taking part in an initial cognitive-motivational interview with the Staff Selection Manager and in a subsequent technical interview with the Function/Organizational Structure Manager, in order to check the skills declared by the candidate. Additional verification tools include exercises and tests.

5.3.3. TRAINING REQUIREMENTS

Camerfirma personnel undertaking duties of trust must have been trained in accordance with the CP. There is a training plan that is part of the ISO/IEC 27001 controls.

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.

Camerfirma prevents anyone from individually affecting or altering system's global security or carrying out unauthorized activities, the operational management of the system is entrusted to different resources, each with separate and well-defined tasks. The personnel in charge of certification service design and provision are Camerfirma employees selected for his experience in designing, implementing and managing IT services and for their reliability and confidentiality. Training sessions are periodically scheduled to familiarize them with the assigned tasks. In particular, training courses are held to provide all the necessary skills (technical, organizational and procedural) to carry out the assigned tasks before staff start their operational tasks.

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.

At the beginning of each year, Camerfirma training requirements are analyzed in order to define the training courses to be held during the year. The analysis is based on following steps:

- Meeting with management to collect data on the training requirements needed to achieve business objectives;
- Feedback from the area managers in order to identify the specific training needs from each area;
- Forwarding of collected data to Corporate Management for Training Plan closing and approval.

Once defined, the Camerfirma Training Plan is shared inside the company.

5.3.5. JOB ROTATION FREQUENCY AND SEQUENCE

On-site working or agile working (smart working) hours are distributed over an 8:00 a.m. to 7:00 p.m. time slot from Monday to Friday.

Supervision of the production environment at night and on public holidays is ensured by means of an on-call rotation plan drawn up by the Security Officer. Depending on the need, interventions may be carried out remotely, remote intervention, or require access to the premises.

Provided that the necessary technical and professional requirements are met, Camerfirma and InfoCert ensure that as many workers as possible are on call, giving priority to employees who request it.

5.3.6. SANCTIONS FOR UNAUTHORIZED ACTIONS

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

Camerfirma sanctions are imposed in accordance with the Workers' Statute and applicable collective agreement, *Oficinas y Despachos*.

5.3.7. INDEPENDENT CONTRACTOR REQUIREMENTS

Camerfirma 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 CA 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.

Camerfirma requirements for access to non-employee personnel is governed by a specific corporate policy.

5.3.8. DOCUMENTATION SUPPLIED TO PERSONNEL

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

This documentation is in an internal repository accessible by any Camerfirma employee; the repository contains a list of documents that must be known and complied with.

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

Upon Camerfirma recruitment, employees must provide a copy of a valid identity document, as well as his/her valid health number. Subsequently, they will be required to complete and sign a written consent to the processing of personal data and a confidentiality agreement, and to review Camerfirma Code of Ethics and Privacy Policy.

5.4. AUDIT LOGGING PROCEDURES

CA management and certificate life-cycle records are collected in the Audit Log as required by the eIDAS Regulation.

5.4.1. TYPES OF EVENTS RECORDED

Archived records include security events, startup and shutdown events, system crashes and hardware failures, firewall and router activity, and PKI system access attempts.

All the data and documents used during identification and acceptance of the Subscriber requests are retained, including copies of ID documents, contracts, business registration excerpts etc.

Certificate registration and life-cycle events are also recorded. These include certificate issuance and re-key requests, certificate registration, generation, distribution and possibly revocation.

All events concerning the personalization of the signature device are recorded.

All physical accesses to high security premises where the CA machines reside are recorded.

All logical accesses to the CA applications are recorded.

All signature device customization events are also archived. Each event is saved with its system date and time.

5.4.2. FREQUENCY OF PROCESSING LOG
Data collection, clustering and archiving on InfoCert preservation system occur monthly.

5.4.3. RETENTION PERIOD FOR AUDIT LOGS
The Audit Log is retained by the CA for 20 years.

5.4.4. PROTECTION OF AUDIT LOG
Audit Log protection is ensured by the InfoCert electronic document preservation system, accredited by AgID in accordance with current legislation.

5.4.5. AUDIT LOG BACKUP PROCEDURES
The InfoCert electronic document preservation system implements backup policies and procedures that are compliant with the requirements of its security manual.

5.4.6. AUDIT COLLECTION SYSTEM (INTERNAL VS. EXTERNAL)
Event logs are collected through ad hoc automatic procedures and archived in the InfoCert preservation system according to the methods described in the InfoCert preservation system security manual.

5.4.7. NOTIFICATION TO EVENT-CAUSING SUBJECT
Not stipulated.

5.4.8. VULNERABILITY ASSESSMENTS
InfoCert performs periodic System vulnerability assessments and penetration tests. Based on the results, all the necessary countermeasures are implemented to secure applications.

5.5. RECORDS ARCHIVAL

5.5.1. TYPES OF RECORDS ARCHIVED
The following information that are part of the certificate's life cycle are stored by the CA or RAs:

- Any CA and qualified centralized module audit data.
- Any data related to certificates, including identification, authentication and agreements.
- Requests to issue and revoke certificates.
- All the certificates and CRLs issued by the CAs.
- All the OCSP service requests and responses.

5.5.2. RETENTION PERIOD FOR ARCHIVE
The CAs preserves the documentation detailed in section 5.5.1 for at least 15 years after the expiration date of any certificate based on that documentation.

5.5.3. PROTECTION OF ARCHIVE
Protection is ensured by the InfoCert preservation system, accredited by AgID.

5.5.4. ARCHIVE BACKUP PROCEDURES
InfoCert document preservation system implements backup policies and procedures that are compliant with the requirements of its security manual.

5.5.5. REQUIREMENTS FOR TIME-STAMPING OF RECORDS

Archived records are dated with a reliable source by the systems which generate them.

5.5.6. ARCHIVE COLLECTION SYSTEM (INTERNAL OR EXTERNAL)

Records are collected through specific automatic procedures and archived in the InfoCert-compliant document preservation system according to the methods described in its security manual.

5.5.7. PROCEDURES TO OBTAIN AND VERIFY ARCHIVE INFORMATION

Data are all stored in a compliant preservation system on which regular accurate checks on the status of the system and the integrity of the data are carried out. Data are displayed in accordance with the relevant standards.

5.6. KEY CHANGEOVER

The CA's keys, Root or Intermediate CA, will be changed before the CA's certificate expires. The old CA's private key can only be used to sign CRLs as long as there are active certificates issued by the old CA, that is, signed with the old CA's private key. A new CA certificate is generated with the new CA public key and a CN, common name, different from the old CA certificate.

A CA's keys and/or certificate are also changed when there is a change to cryptographic technology, that is, algorithms, key size, etc., that requires it, or to comply with the requirements of applicable standards and legislation.

Each CA key changeover results in an amendment of this CPS and is notified to *Ministerio de Asuntos Económicos y Transformación Digital*.

5.7. COMPROMISE AND DISASTER RECOVERY

5.7.1. INCIDENT AND COMPROMISE HANDLING PROCEDURES

The CAs, Root and Intermediate CAs, have described their incident handling procedures in InfoCert and Camerfirma ISO 27000-certified information security management system (ISMS). Any incident detection is immediately followed by incident analysis, detection of corrective countermeasures and drawing up of a report by the service manager. In accordance with Article 19 of the eIDAS Regulation, a copy is also sent to the Supervisory Body.

At the time the incident continues no digital certificates will be issued.

5.7.2. COMPUTING RESOURCES, SOFTWARE, AND/OR DATA ARE CORRUPTED

In the event of a failure of the HSM secure signature device containing CA keys, an appropriately saved and stored certification backup key is used instead, and there is no need to revoke the corresponding Intermediate CA certificate or to distrust the corresponding Root CA certificate.

Software and data are subject to regular backups as provided by Camerfirma and InfoCert internal procedures.

5.7.3. ENTITY PRIVATE KEY COMPROMISE PROCEDURES

A CA, Root or Intermediate CA, private key compromise is regarded as a particularly critical event as it invalidates issued certificates and the revocation status information signed with that key. Therefore, special focus is given to protection of the CAs private key and to all system development and maintenance activities that may have an impact on it.

Although it is a rare event, InfoCert and Camerfirma have set up a detailed procedure to be followed within the ISO 27000 certified ISMS.

Once the compromise of a CA private key has been ascertained, Camerfirma will promptly proceed:

- to notify the Spanish Supervisory Body within the next 24 hours,
- to notify RAs and customers, whether Subjects/Signatories or Subscribers, Relying Parties and other entities with which it has agreements or other types of relationships, through direct communication where possible, and through communication on the Camerfirma website,
- to notify that the certificates and information relating to the revocation status that are signed using this CA private key are not valid,
- to revoke the affected certificates,

- to reliably provide information on the certificates revocation status, signed using a different CA private key,
- and to proceed, if necessary, with the issuance and accreditation of a new Intermediate or Root CA.

5.7.4. BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER

Camerfirma and InfoCert have adopted the procedures required to ensure continuity of its service even in highly critical or disaster situations.

5.8. CA OR RA TERMINATION

Before Camerfirma ceases its activity as a TSP issuing certificates under this CPS:

- It shall provide the required funds, via a budget item and a public liability insurance policy, to complete the transfer and/or termination processes.
- It shall notify the Supervisory Body, at least three months in advance, of the termination of its activity as a TSP issuing certificates and, if applicable, of the reliable party that it will transfer any obligations (see below).
- It shall notify all Subscribers, Subjects/Signatories, Responsible, Relying Parties and other entities with which it has agreements or other types of relationships, of termination of activity at least two months in advance.
- It shall publish on its website or any other means accessible to users, the pertinent information concerning the conclusion of its operations.
- It shall revoke any authorisation from subcontracted entities to act on behalf of any affected Camerfirma CA under this CPS in the certificate issuance procedure.
- It shall continue to carry out its obligations related to maintaining registration information, revocation status information and event log archives, and to providing revocation status information, for the established time period indicated to Subscribers, Subjects/Signatories and Relying Parties, or it will transfer these obligations to a reliable party.
- It shall notify the Supervisory Body of any bankruptcy proceedings against the TSP, as well as of any other circumstance that will prevent the activity of Camerfirma as TSP.
- It shall terminate any affected Camerfirma CA under this CPS (see below).

All these activities will be included in detail in the Camerfirma Termination plan.

Before Camerfirma terminates any CA under this CPS:

- In the event that the termination of the CA includes its replacement by a new CA or by another existing CA, it shall notify all Subscribers and Subjects/Signatories, offering them to issue their certificates with the other CA.
- It shall revoke all active certificates issued by this CA.
- It shall issue and publish a last CRL, including revoked expired certificates, with the nextUpdate field equal to "99991231235959Z".
- If the CA is an Intermediate CA, it shall revoke the CA certificate by the corresponding issuing CA (usually a Root CA).
- It shall destroy the CA private key.
- It shall notify the Supervisory Body and other entities with which it has agreements or other types of relationships, of the termination of the CA and the actions carried out.

6. TECHNICAL SECURITY CONTROLS

6.1. KEY PAIR GENERATION AND INSTALLATION

6.1.1. KEY PAIR GENERATION

In order to provide its service, the CA needs to generate a key pair used to sign the Subject certificates.

Such keys are generated solely by staff specifically in charge of this function. Key and signature generation takes place within dedicated and certified cryptographic modules, as required by current legislation.

Protection of the CA private key is ensured by the key generation and usage cryptographic module. The private key can only be generated if two key generation employees are simultaneously present. Key generation takes place in the presence of the service manager.

CA private keys are duplicated for the sole purpose of being recovered after secure signature device breakdown. Duplication takes place through a controlled procedure by which the key and its context are duplicated on multiple devices as required by HSM device safety criteria.

The cryptographic module used for key generation and signature complies with requirements that ensure:

- Compliance of the key pair with minimum requirements imposed by the generation and verification algorithms used;
- A fair probability of generation of possible pairs;
- Identification of the Subject activating the generation procedure;
- That signature generation takes place inside the device so that the value of the private key being used cannot be intercepted.

6.1.1.1. CREATING THE SIGNATORY'S KEY PAIR

Asymmetric keys are generated within a secure signature creation device (SSCD or QSCD, HSM type) provided by Camerfirma using native features provided by the devices themselves.

The keys have a minimum length of 2.048 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 CA and Intermediate CAs keys use a cryptographic device that complies with FIPS-104-2 level 3 or EAL4+ specifications.

6.1.2. PRIVATE KEY DELIVERY TO SUBSCRIBER

Private keys are contained in the cryptographic device, which can be either an SSCD or a QSCD.

By delivering the cryptographic device to the Subject, the latter comes into full possession of the private key, which he can only use by entering a PIN that is known exclusively to him.

Where the registration procedure is performed in the presence of the Subject, the device is delivered as soon as the keys are generated.

If the registration process is not performed in the presence of the Subject, the device is delivered according to the methods provided by the contract, paying attention that the device and its instructions for use travels on different channels or are delivered to the Subject at two different moments in time. In some cases, the Subject may already have the devices available, as they have been delivered in advance according to safe procedures and against identification of the Subject.

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

See Section 2.2.3.

6.1.5. KEY SIZES

The certification asymmetric key pair is generated within the cryptographic hardware devices mentioned above.

The Root CA and Intermediate CAs keys can be:

- RSA asymmetric keys with a length of not less than 4.096 bits;
- EC asymmetric keys on one of the elliptic curves provided by ETSI document TS 119 312 – Cryptographic Suites with a length of not less than 256 bits.

The end entity certificate keys may be:

- RSA asymmetric keys with a length of not less than 2.048 bits;
- EC asymmetric keys on one of the elliptic curves provided by ETSI TS 119 312 – Cryptographic Suites document with length not less than 256 bits.

6.1.6. PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING

Devices are certified according to high security standards (see section 6.2.1) and ensure that the public key is correct and random. Prior to issuing a certificate, the CA verifies that the public key has not been used before.

6.1.7. KEY USAGE PURPOSES (AS PER X.509 V3 KEY USAGE FIELD)

Key usage purposes are determined by the KeyUsage extension, as defined in the X509 standard. For certificates covered in this CPS, the permitted uses are “contentCommitment”, “digitalSignature” and/or “keyEncipherment”.

6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1. CRYPTOGRAPHIC MODULE STANDARDS AND CONTROLS

Cryptographic modules used by Camerfirma for certification keys (CA) and OCSP responder are validated FIPS 140 Level 3 and Common Criteria (CC) Information Technology Security Evaluation Assurance Level (EAL) EAL 4+ Type 3 (EAL 4 Augmented by AVA_VLA.4 and AVA_MSU.3) in Europe.

QSCD SmartCard or Token devices used by Camerfirma are validated CC EAL 4+ Type 3 (EAL 4 Augmented by AVA_VLA.4 and AVA_MSU.3), or EAL5 Augmented by ALC_DVS.2, AVA_VAN.5.

QSCD Cloud devices are certified FIPS 140 Level 3 and/or CC EAL4+.

Camerfirma shall check compliance of used QSCD SmartCard or Token devices and QSCD Cloud devices with the eIDAS Regulation either with the latest list of these devices published by the EU or by notification from the Supervisory Body. If Camerfirma detects in these checks that any of these devices is not considered a QSCD anymore, Camerfirma shall revoke all active certificates in which the private key is in that device.

6.2.2. PRIVATE KEY (N OUT OF M) MULTI-PERSON CONTROL

Access to devices containing the certification keys can only occur when two users are simultaneously authenticated.

6.2.3. PRIVATE KEY ESCROW

Not stipulated.

6.2.4. PRIVATE KEY BACKUP

The CA private keys backup is contained in a safe whose access code is solely given to personnel who do not have access to HSM devices. Key restoration therefore requires that both personnel in charge of the device and employees who have access to the safe are present at the same time.

6.2.5. PRIVATE KEY ARCHIVAL

The CA private keys backup is contained in a safe whose access code is solely given to personnel who do not have access to HSM devices. Key restoration therefore requires that both personnel in charge of the device and employees who have access to the safe are present at the same time.

6.2.6. PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE

Not stipulated.

6.2.7. PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE

The certification private keys are generated and stored in a secure area of the cryptographic device, managed by the certifier, which prevents its export. In addition, if an attempt at forcing the protection occurs, the operating system of the device blocks the device or makes itself unreadable.

6.2.8. METHOD OF ACTIVATING PRIVATE KEY

The certification private keys are activated by the CA software in dual control, that is by two employees with specific roles and in the presence of the service manager.

The Subject or Subscriber acting as legal representative of a legal person is responsible for protecting his private key with a strong password to prevent unauthorized use. To activate the private key, the Subject must authenticate himself.

6.2.9. METHOD OF DEACTIVATING PRIVATE KEY

Not stipulated.

6.2.10. METHOD OF DESTROYING PRIVATE KEY

Camerfirma and InfoCert staff in charge of this role deals with the destruction of the CA private keys when the certificates expire or are revoked, according to security procedures provided by security policies and device manufacturer specifications.

6.2.11. CRYPTOGRAPHIC MODULE RATING

Not stipulated.

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1. PUBLIC KEY ARCHIVAL

Not stipulated.

6.3.2. CERTIFICATE OPERATIONAL PERIODS AND KEY PAIR USAGE PERIODS

A certificate validity period shall be determined based on:

- The state of technology;
- The state of the art for cryptographic technologies;
- The intended use of the certificate.

Currently, the CA certificates are valid for not more than 24 years. Certificates issued to natural or legal persons are valid for not more than 39 months.

6.4. ACTIVATION DATA

See sections 4.3.3 and 6.3.

6.5. COMPUTER SECURITY CONTROLS

Camerfirma and InfoCert uses reliable systems to provide certification services. Camerfirma and InfoCert 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.

6.5.1. SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS

The operating system of computers used in certification activities involved in key generation, certificate generation and certificate registry management are hardened, i.e. they are configured to minimize the impact of any vulnerabilities by eliminating features that are not required for CA operation and management.

System administrators appointed for this purpose in accordance with applicable regulations shall access the system by means of a root on demand application, that enables root user privileges to be used only after individual authentication. Each access is traced, logged and stored for 12 months.

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 SmartCard or Token certified as a qualified signature creation device in compliance with Appendix II of eIDAS.

As regards hardware devices:

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

With respect to the devices used in the *Cloud QSCD* management: The device that stores these keys is FIPS-104-2 level 3 or EAL4+ certified and authorized by the Supervisory Body for services catalogued 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.

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.

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.

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.

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

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.

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

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

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.

6.6.2.4. ACCESS SYSTEM MANAGEMENT

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

- There are controls based on firewalls, antivirus and IDS with high availability.
- Sensitive data is protected via cryptographic methods or strict identification access controls.
- Camerfirma has established a documented procedure to process user registrations and cancellations and a detailed access policy in its security policy.
- Camerfirma has implemented procedures to ensure tasks are undertaken in accordance with the roles policy.
- Each person is assigned a role to carry out certification procedures.
- 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 SmartCard or Token based authentication of an authorised administrator's applications. The audit log systems generate evidence that guarantees non-repudiation of the action taken by the CA administrator.
- Revocation status: The revocation status application includes access control based on authentication via certificates to prevent attempts to change the revocation status information.

6.6.2.5. MANAGING THE CRYPTOGRAPHIC HARDWARE LIFECYCLE

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

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

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

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

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

The cryptographic hardware device is only handled by trustworthy personnel.

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

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

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

6.6.3. LIFE CYCLE SECURITY CONTROLS

Not stipulated.

6.7. NETWORK SECURITY CONTROLS

For its certification service, Camerfirma and InfoCert has designed a network security infrastructure based on firewalling mechanisms and on the SSL protocol to provide a secure channel between the RAs and the certification system, and between the certification system and administrators/operators.

Camerfirma and InfoCert systems and networks are connected to the Internet in a controlled way by means of firewall systems that allow splitting up the connection into progressively more secure areas: Internet networks, DMZ (Demilitarized Zone) or Perimeter Networks, and Internal networks. All traffic flowing between areas is subject to acceptance by the firewall, based on a set of established rules. Firewall rules are designed based on "default deny" (what is not expressly permitted is forbidden by default, or the rules will only allow what is strictly necessary for the application

to properly work) and "defense in depth" (increasing layers of defense are arranged, first at the network level, through successive firewall barriers, and finally at system level through hardening) principles.

6.8. TIME-STAMPING

To implement a precise, accurate and reliable system time reference used by all systems involved in the generation of certificates and CRLs issued by the Intermediate CAs, the operational solution is based on physical appliances that act as NTP servers synchronized through the signals provided by the GPS and GLONASS satellite systems. NTP servers can also use INRIM NTP servers as an additional time reference. The whole architecture is in high availability.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1. CERTIFICATE PROFILE

Certificate profiles complies with IETF RFC 5280.

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

Camerfirma publishes details of the basic certificate fields and certificate extensions of the certificate types issued in hierarchies described in this CPS in https://policy21.camerfirma.com.

7.1.1. VERSION NUMBER

Camerfirma issues X.509 certificates Version 3.

7.1.2. CERTIFICATE EXTENSIONS

See section 7.1.

7.1.3. ALGORITHM OBJECT IDENTIFIERS

The signature algorithm object identifier would be:

- 1.2.840.113549.1.1.11 - sha256WithRSAEncryption
- 1.2.840.113549.1.1.12 - sha384WithRSAEncryption
- 1.2.840.113549.1.1.13 - sha512WithRSAEncryption

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

7.1.4. NAME FORMAT

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

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

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

The exact semantics of the names are described in the profile records. See section 7.1 for information about profile records.

7.1.5. NAME CONSTRAINTS

No stipulation.

7.1.6. CERTIFICATION POLICY OBJECT IDENTIFIER

All certificates have a policy identifier that starts from the base 1.3.6.1.4.1.17326.

7.1.7. USAGE OF POLICY CONSTRAINTS EXTENSION
No stipulation.

7.1.8. POLICY QUALIFIERS SYNTAX AND SEMANTICS
No stipulation.

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 section 7.1.6.

7.2. CRL PROFILE
Camerfirma CRLs complies with IETF RFC 5280.

The CRLs are signed by the CA that issued the certificates.

The CRL of the Root CA 'CAMERFIRMA ROOT 2021' has a validity of 365 days.

The CRLs of the Intermediate CA 'AC CAMERFIRMA QUALIFIED CERTIFICATES - 2021' have a validity of 24 hours.

7.2.1. VERSION NUMBER
The CRLs issued by Camerfirma are version 2.

7.2.2. CRL AND CRL ENTRY EXTENSIONS
All the CRLs issued by Camerfirma include the following CRL extensions:

- CRL Number (OID 2.5.29.20), as defined in IETF RFC 5280.
- Authority Key Identifier (OID 2.5.29.35), as defined in IETF RFC 5280 and including only the keyIdentifier field.

All the CRLs issued by the Intermediate CA 'AC CAMERFIRMA QUALIFIED CERTIFICATES - 2021' include the following CRL extensions:

- ExpiredCertsOnCRL (OID 2.5.29.60), as defined in ISO/IEC 9594-8/Recommendation ITU-T X.509 and set to the CA's certificate "notBefore" time and date value.
- Issuing Distribution Point (OID 2.5.29) as defined in IETF RFC 5280.

The CRLs include the following CRL entry extension:

- Reason Code (OID 2.5.29.21), as defined in IETF RFC 5280.

7.3. OCSP PROFILE
The OCSP responses profile complies with IETF RFC 6960.

Camerfirma shall include the reason for revocation in the information on each revoked certificate in the OCSP responses.

The OCSP responder certificates profile complies this CPS section 7.1.

7.3.1. VERSION NUMBER
Conforming IETF RFC 6960.

7.3.2. OCSP EXTENSIONS
Camerfirma Root CAs and Intermediate CAs include in OCSP responses the following extensions:

- Nonce (OID 1.3.6.1.5.5.7.48.1.2), as defined in IETF RFC 6960 and as a non-critical extension.
- Archive CutOff (OID 1.3.6.1.5.5.7.48.1.6), as defined in IETF RFC 6960, set to the CA's certificate "notBefore" time and date value and as a non-critical extension.
- Extended Revoked Definition (OID 1.3.6.1.5.5.7.48.1.9), as defined in IETF RFC 6960 and as a non-critical extension.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1. FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

Camerfirma will carry out the necessary audits periodically. This periodicity is mainly on an annual basis.

8.2. IDENTITY/QUALIFICATIONS OF ASSESSOR

The audits are conducted by independent external companies that are widely renowned in computer security, information systems security and compliance audits for CAs.

8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The contracted auditing companies are independent and reputable companies with specialized IT audit departments that manage digital certificates and trust services, which rules out any conflict of interest that may affect their activities in relation to the CAs.

There is no financial or organizational association between the auditing firms and the CAs.

8.4. TOPICS COVERED BY ASSESSMENT

In general terms, the audits verify:

- That Camerfirma has a system that guarantees service quality.
- That Camerfirma complies with the requirements of the CPs that regulate the issuance of the different digital certificates.
- That the CPS is in keeping with the provisions of the CPs, with the agreement of the Policy Authority and with the requirements of current legislation.
- That the CAs properly manages the security of its information systems.

The elements audited are:

- The CAs, RAs and validation services.
- Information systems.
- Data centers.
- Documentation required for each type of certificate.
- Verification that the RA operators know CAs' CPS.

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 to address the shortcomings.

If the audited entity is unable to develop and/or implement the plan within the requested timeframe, or if the deficiencies pose an immediate threat to the security or integrity of the system, the PA shall be notified immediately, and may take the following actions:

- Cease operations temporarily.
- Revoke the corresponding certificate/s and restore the infrastructure.
- Terminate service to the Entity.
- Other complementary actions as necessary.

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.

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 in Camerfirma's website.

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

9.1.2. CERTIFICATE ACCESS FEES

Access to the public registry of issued certificates is free of charge.

9.1.3. REVOCATION OR STATUS INFORMATION ACCESS FEES

Camerfirma provides free access to information relating to the status of certificates via CRL or via OCSP service.

9.1.4. FEES FOR OTHER SERVICES

Access to the content of this CPS is free-of-charge on Camerfirma's website https://policy21.camerfirma.com.

9.1.5. REFUND POLICY

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 Spanish 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 TSP, 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 Relying Party and third parties, for a minimum amount of 1,500,000 € plus 500,000 € for each eIDAS qualified service.

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 explicit written consent from the entity or organization that classified this information as confidential, unless established by law.

Camerfirma has established an information and file processing policy in accordance with its confidentiality, which anyone accessing confidential information must sign.

Camerfirma complies with current legislation on personal data protection:

- Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (RGPD).
- Spanish Organic Law on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD).

9.3.2. INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION

Camerfirma deems the following information not confidential:

- The contents of this CPS and CP.
- The information included in the certificates, CRLs and OCSP responses.

9.3.3. RESPONSIBILITY TO PROTECT CONFIDENTIAL INFORMATION

Camerfirma is responsible of the protection of the confidential information generated or communicated during all operations. RAs are responsible for protecting confidential information that has been generated or stored by their own means.

For end entities, the Subject or the Responsible of the certificate 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.

9.4. 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 EU Regulation RGPD. In this sense, this document serves, in accordance with Law 6/2020 of November 11, regulating certain aspects of electronic trust services (Article 8) and the eIDAS Regulation (Article 24.2.f) as a security document.

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 LOPDGDD/RGPD legislation.

9.4.4. RESPONSIBILITY TO PROTECT PRIVATE INFORMATION

It is the responsibility of the data 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

Those described in article 6.1 of the RGPD or any other legal provision that is applicable.

9.5. INTELLECTUAL PROPERTY RIGHTS

Camerfirma owns the intellectual property rights on this CPS and CPs, and on the electronic certificates it issues except if different agreement has been reached.

9.6. REPRESENTATIONS AND WARRANTIES

9.6.1. CA REPRESENTATIONS AND WARRANTIES

9.6.1.1. CA

In accordance with the stipulations of this CPS and 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 CPs.
- Protect its private keys and keep them secure.
- Issue certificates in accordance with this CPS and CPs 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 content defined by current law for qualified certificates.

- Publish issued certificates in a directory, respecting all legal provisions regarding data protection.
- Revoke certificates in accordance with this Policy and publish the revocations in the CRLs.
- Inform Subjects and other interested person about the revocation of their certificates, on time and in accordance with current law.
- Publish this CPS and CPs on its website.
- Report changes to this CPS and CPs to the Subjects, the Subscriber and its associated RAs.
- Do not store or copy the Subject's signature creation data except for encryption certificates and when it is legally provided for or allowed to be stored or copied.
- Protect data used to create the signature while in its safekeeping, if applicable.
- Establish data creation and custody systems in the aforementioned activities, protecting data from being lost, destroyed or forged.
- Keep data relating to the issued certificate for the minimum period required by current law.

Camerfirma's responsibility:

Article 10 of the Law 6/2020 on Trust Services establishes that:

"*Trusted electronic service providers shall assume all liability to third parties for the activities of persons or other providers to whom they delegate the performance of any or some of the functions necessary for the supply of trusted electronic services, including identity verification activities prior to the issuance of a qualified certificate*."

Article 13 of the eIDAS Regulation provides:

"1. Without prejudice to the provisions of paragraph 2, trusted service providers are responsible for damages caused intentionally or negligently to any natural person or legal entity for breach of its obligations under this Regulation.

The burden of proof of intent or negligence of an unqualified trusted service provider corresponds to the natural person or legal entity claiming the damages that the first paragraph refers to.

The intent or negligence of a qualified trusted service provider is presumed unless the qualified trusted service provider proves that the damage referred to in the first paragraph occurred without intent or negligence on its part.

2. When a service provider duly informs its customers in advance about the limitations of the use of the services provided and these limitations are recognisable to a third party, the trusted service provider is not responsible for damages caused by use of services beyond the limitations stated.

3. Paragraphs 1 and 2 shall apply in accordance with Spanish liability regulations."

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

In this sense, Camerfirma is the only partly responsible for (i) issuing the certificates, (ii) managing them throughout their lifecycle and (iii) in particular, if necessary, in the event of 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 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 this CPS.

9.6.2. RA REPRESENTATIONS AND WARRANTIES

RAs are entities that the CAs appoints to register and approve certificates; therefore, the RAs also carry out the obligations defined in this CPS and CP for issuing certificates and in accordance with current law, particularly to:

- Adhere to the provisions of this CPS and CP applicable to each kind of issued certificate.
- Protect their private keys that are used for exercising their functions.
- Respect the terms of the agreement signed with the CA.
- Respect the Terms and Conditions signed by the Subject and/or Subscriber.

Regarding the life cycle of certificates:

- Before the issuance of the certificate:
  - Check the identity of the Subject and/or Subscriber of certificate according to the methods defined in this CPS.
  - Check the accuracy and authenticity of information provided by the Applicant or the Responsible.
  - Inform the Subject and/or Subscriber about his/her obligations, about the way to keep the data and device of electronic signature creation, and data to accede to them, and about the process he/she has to follow in case of misuse or lost the certificate or device, limits of use, liability, etc. and where he/she can access to consult CPS, CPs and Terms and Conditions.
  - Manage and provide the Subject or the Subscriber or the Responsible with the certificate according to CPS and CP.
  - If applicable, deliver the corresponding cryptographic device.
  - Formalize the Terms and Conditions and other contractual documents with the Subject and/or Subscriber on an analogic manner or using digital tools that enable the conservation of the formal acceptation.
- After the issuance:
  - Keep the documents provided by the Subject and/or Subscriber and signed Terms and Conditions in physical or digital archive file for the period required by current law.
  - Inform the CA about the causes for revocation, when known.

Therefore, the RAs are responsible for any consequences due to non-compliance of registration duties, and undertake to adhere to this CPS, which the RAs must keep perfectly controlled and which they must use as guidelines.

In the event of a claim from a Subject, Subscriber or Relying party, the CAs 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 CAs can hold the RAs liable for the consequences, in accordance with the agreement signed with the RAs.

To avoid breaches of RAs obligations, the CAs control periodically the RAs activity and audit at least each two (2) years 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 RAs in virtue of breaches of the delegated entities such as points of physical verification (PPV), without prejudice to their right to contest them.

9.6.3. SUBSCRIBER REPRESENTATIONS AND WARRANTIES

9.6.3.1. SUBSCRIBER

The Subscriber of a certificate shall be bound to comply with the provisions of the regulations and in addition to:

- Accept the Terms and conditions imposed by the provider.
- Notify the RA or the CA of any change in the data provided for the issuance of the certificate during its period of validity.
- Inform the RA or the CA as soon as possible of the existence of any cause of revocation.

9.6.3.2. APPLICANT

The Applicant of a certificate shall be bound to comply with the provisions of the regulations and in addition to:

- To provide the RA with the necessary information to carry out a correct identification.
- Guarantee the accuracy and veracity of the information provided.

- Notify the RA or the CA of any change in the data provided for the issuance of the certificate during its period of validity.
- Inform the RA or the CA as soon as possible of the existence of any cause of revocation.
- Provide the information of the Subject (Signatory)/Applicant/Responsible under the rules imposed by the law of data protection.

9.6.3.3. SUBJECT/HOLDER/RESPONSIBLE

The Subject/Holder and the Responsible if different than the Subject/Holder, will be obliged to comply with the provisions of the regulations in force and in addition to:

- Accept the terms and conditions imposed by the provider.
- Use the certificate as established in the present CPS and CPs.
- Respect the provisions of the documents signed with Camerfirma, the CAs and the RAs.
- To make use of the digital certificate as personal and non-transferable and custody of the private key activation data in a diligent manner. Subject/Holder and Responsible will be solely responsible to Entity he/she represents and Relying Party in case of not having authorization, and for the consequences if a misuse or not properly control.
- Inform the RA or the CA as soon as possible of the existence of any cause for revocation.
- Notify the RA or the CA of any inaccuracy or change in the data provided for the creation of the certificate during its period of validity.
- Not to use the private key neither the certificate from the moment in which it is requested or it is warned by the CA or the RA of the revocation of the same one, or once the term of validity of the certificate has expired.
- To authorize the CA and RA to proceed to the treatment of the personal data contained in the certificates, in connection with the purposes of the electronic relation and, in any case, to fulfil the legal obligations of verification of certificates.
- Be responsible that all the information included, by any means, the request for the certificate and the certificate itself is accurate, complete for the purpose of the certificate and is updated at all times.
- Immediately inform the CA or RA of any inaccuracies in the certificate detected once it has been issued, as well as any changes in the information provided by the issuance of the certificate.
- In the case of certificates in a hardware device, in the event that it loses its possession, make it known to the RA or the CA as soon as possible and, in any case, within 24 hours following the production of the aforementioned circumstance, regardless of the specific event that originated it or the actions that it may eventually exercise.
- Not to use the private key, the electronic certificate or any other technical support provided by the CA or RA to carry out any transaction prohibited by the applicable law.

The Subject/Holder and Responsible should also be especially diligent in the safekeeping of the private key and the qualified signature creation device, in order to avoid unauthorized use.

9.6.4. RELYING PARTY REPRESENTATIONS AND WARRANTIES

It shall be the obligation of the Relying Party to comply with the provisions of the regulations in force and, in addition:

- Verify the status of the certificates, either by consulting the CRLs or the OCSP services, and the non-expiration of the certificates before performing any operation based on them.
- To know and be subject to the applicable guarantees, limits and responsibilities in the acceptance and use of the certificates in which it trusts, and to accept to be subject to the same ones. In case of certificates for a Special Representative of a Legal Entity or a Non-legal Entity that involve a representation relationship based on a special power of attorney or private document with limited faculties, relying parties should check the limits of such faculties.
- Verify that the certificate is qualified by checking that the certificate has been signed with the private key associated with a valid CA certificate of Camerfirma included in the Spanish Trusted List which is in force, in accordance with the provisions of article 22 of the eIDAS Regulation and in the Commission's Execution Decision (EU) 2015/1505, of September 8, 2015, which establishes the technical specifications and formats related to trusted lists in accordance with Article 22(5) of eIDAS Regulation.

9.6.5. REPRESENTATIONS AND WARRANTIES OF OTHER PARTICIPANTS

In the case of those certificates that imply a link between a natural person and an Entity, the Entity will be obliged to request to the CA or the RA the revocation of the certificate when the natural person ceases to be linked to the Entity.

9.7. DISCLAIMERS OF WARRANTIES

In accordance with current law, the responsibility assumed by the CAs and the RAs does not apply in cases in which certificate misuse is caused by actions attributable to the Applicant, Subject, Responsible and the Relying 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 CA or the RA 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 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 Relying 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 number of transactions, or when it does not consider the certificate's validity situation.
- Damages caused to the Subject, Entity or Relying parties due to the inaccuracy of the data included in the digital certificate, if these data have been evidenced through a public document registered in a public register, if required.
- An inadequate or fraudulent use of the certificate in case the Subject/Holder and/or the Responsible has transfer it or authorized its use in favor of a third person being the sole responsibility of the Subject/Holder and the Responsible the control of the keys associated with the 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 , the CPS and/or the CPs.
- Improper or fraudulent use of certificates, CRLs or OCSP responses.
- Use of the information contained in the certificates, CRLs or OCSP responses.
- Damages caused during verification of the causes for revocation.
- 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

9.8.1. CA LIMITATIONS OF LIABILITY

Camerfirma is liable for non-compliance with the provisions of the CPS and, where applicable, with the provisions of the eIDAS Regulation and Law 6/2020.

Camerfirma does not guarantee the cryptographic algorithms and standards used and will not be liable for damage caused by external attacks on them, provided that due diligence has been applied according to the state of the art at any given time, and it has acted in accordance with the provisions of this CPS and the eIDAS Regulation and Law 6/2020.

Camerfirma shall be liable for any damage caused to the Subscriber or Subject or any Relying party, provided there is fraud or major negligence, with regard to:

- The guarantee that the public and private key work in combination and in a complementary manner.
- The accuracy of the information included in the certificate on the date of issue, provided that this matches the authenticated information.
- The correspondence between the certificate requested and the certificate delivered.
- Any liability established by the applicable legislation in force.

9.8.2. RA LIMITATIONS OF LIABILITY

The RA shall be fully responsible for the identification and authentication procedure of Subscribers, Applicants, Subject or Responsible. It shall do so in accordance with the provisions of this CPS.

If the generation of the key pair is not performed in the presence of the Subject/Holder or the Responsible, the RA shall be responsible for the custody of the keys until they are delivered to the Subject/Holder or the Responsible.

9.8.3. SUBSCRIBER/APPLICANT/SUBJECT/HOLDER/RESPONSIBLE LIMITATIONS OF LIABILITY

It is the full liability of the Subscriber/Applicant/Subject/Holder/Responsible to comply with the obligations stipulated in this document and in the legal documents signed by them.

9.8.4. CAMERFIRMA LIMITATIONS OF LIABILITY

Camerfirma shall not be liable in any case in the following circumstances:

- State of war, natural disasters, malfunction of electrical services, telematic and/or telephone networks or computer equipment used by the Subscriber/Applicant/Subject/Holder/Responsible, or by Relying parties or any other case of force majeure.
- Where applicable, for improper use of the certificate repositories issued by the CAs.
- Improper use of the information contained in the certificates, in the CRLs or in the OCSP services.
- With regard to the content of the messages or documents signed or encrypted by the certificates.
- With regard to the actions or inactions of the Subscriber/Applicant/Subject/Holder/Responsible:
    - Lack of accuracy or veracity of the information provided to issue the certificate.
    - Delay in notifying the causes for revocation of the certificate.
    - Failure to request the revocation of the certificate when applicable.
    - Negligence in the conservation of its electronic signature creation data, the data for accessing the electronic signature creation data, securing its confidentiality and protecting it against any access or disclosure.
    - Use of the certificate beyond its period of validity or when the CAs notifies the revocation of the certificate.
    - Exceeding the limits on the use of the certificate, as stipulated in the current regulations and in this CPS and CPs or not using it in accordance with the conditions established and communicated to the Subscriber/Applicant/Subject/Holder/Responsible.
- In relation to actions or inactions of the Relying party on the certificate:
    - Failure to verify the restrictions contained in the certificate or in this CPS and CPs regarding its possible uses.
    - Failure to check the expiry date of the certificate stated in the certificate validity extension or failure to verify the digital signature.

9.9. INDEMNITIES

The insurance shall cover all amounts that Camerfirma is legally liable to pay, up to the contracted coverage limit, as a result of any legal proceedings in which its liability may be declared.

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 section 1.5.2.

9.12.AMENDMENTS

9.12.1. PROCEDURE FOR AMENDMENT

Camerfirma 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 Regulation, CA/B Forum, Supervisory Bodies, etc.) or as a result of the optimization of the work cycle. Each new version of this document replaces all previous versions, which remain, however, applicable to the certificates issued while those versions were in force. At least one annual update will be published. These updates will be reflected in the version document history at the end of the document.

Changes that can be made to this document do not require notification except that it directly affects the rights of the Subscriber/Subject/Holder/Responsible/Relying parties, in which case they may be notified within 15 days through Camerfirma web page.

9.12.2. NOTIFICATION MECHANISM AND PERIOD

9.12.2.1. LIST OF ASPECTS

Any aspect of this document can be changed without notice.

9.12.2.2. NOTIFICATION METHOD

Any proposed changes to this document are published immediately on Camerfirma's website https://policy21.camerfirma.com

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

Changes to this document are expressly communicated to third party entities and companies that issue certificates under this CPS and CPs. Especially the changes in this CPS and CP will be notified to the Supervisory Body.

9.12.2.3. PERIOD FOR COMMENTS

The affected Subscriber/Subjects/Responsible and Relying Parties can submit their comments to the policy management organization within 15 days following receipt of notice.

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

In case of any dispute or conflict arising from this CPS and Terms and Conditions, the parties, waiving any other jurisdiction that may correspond to them, submit to the Madrid Courts and Tribunals, except if the claimant is a consumer, so the Judge or Court that corresponds to the consumer's address will be competent.

9.14.GOVERNING LAW

The execution, interpretation, modification or validity of this CPS and CPs is obliged to fulfil the requirements established within current Spanish and European Union law in force at each time.

9.15.COMPLIANCE WITH APPLICABLE LAW

See section 9.14.

9.16.MISCELLANEOUS PROVISIONS

9.16.1. ENTIRE AGREEMENT

The Signatory and Relying parties that rely on the Certificates assume in their entirety the content of this CPS and CPs.

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 individually 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 request indemnification and attorneys' fees from a party for damages, losses and expenses related to such party's conduct. Camerfirma's failure to enforce a provision of this CPS does not eliminate Camerfirma's right to enforce the same provisions later or the right to enforce any other provision of this CPS. To be effective, any disclaimer must be in writing and signed by Camerfirma.

APPENDIX I: DOCUMENT HISTORY

2022-Jan-19	V1.0.0	Initial version