AN INFOCERT COMPANY

CERTIFICATION PRACTICE STATEMENT

CAMERFIRMA 2003-2008-2016

Version 1.3.1

Author: Juan Ángel Martín (Compliance Consultant)

Revised by: Andrés Vázquez (Head of Compliance department)

Approved by (PA): Camerfirma's Legal department

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

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

Language: English

Code: PUB-2022-18-10

SELLO JURIDICO

Firmado digitalmente por SELLO JURIDICO
Fecha: 2022.08.23 14:42:53 +02'00'

INDEX

1 INTRODUCTION

1.1 GENERAL OVERVIEW

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

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

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

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

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

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

Regulation (EU) 910/2014 of the European Parliament and 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) establishes as trust services the following electronic services, which are normally provided for remuneration and consist of: - the creation, verification, and validation of electronic signatures. Certificates relating to these services are included; - the creation, verification, and validation of electronic stamps. The creation, verification, and validation of electronic time stamps. Included are certificates relating to these services; certified electronic delivery. Certificates relating to these services are included; - the creation, verification, and validation of certificates for the authentication of websites, and - the preservation of electronic signatures, seals, or certificates relating to these services.

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

Service	EN general	EN scope	Profiles/Semantics

Creation, verification, and validation of certificates issued to natural persons (including electronic signature certificates and qualified electronic signature certificates, by the eIDAS Regulation)	EN 319 401 v2.3.1 General Policy Requirements for Trust Service Providers	EN 319 411-1 v1.3.1: General Requirements EN 319 411-2 v2.4.1: 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
Creation, verification, and validation of certificates issued to legal persons (including electronic seal certificates and qualified electronic seal certificates, by the eIDAS Regulation)	EN 319 401 v2.3.1 General Policy Requirements for Trust Service Providers	EN 319 411-1 v1.3.1: General Requirements EN 319 411-2 v2.4.1: 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 319 412-3 v1.2.1: Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons EN 319 412-5 v2.3.1: Certificate Profiles; Part 5: QcStatements
Creation, verification, and validation of certificates for the service of creation, verification, and validation of electronic timestamps	EN 319 401 v2.3.1 General Policy Requirements for Trust Service Providers	EN 319 411-1 v1.3.1: General Requirements EN 319 411-2 v2.4.1: Requirements for trust service providers issuing EU qualified certificates EN 319 421 v1.1.1:	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 319 412-3 v1.2.1: Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons EN 319 412-5 v2.3.1: Certificate Profiles; Part 5: QcStatements EN 319 422 v1.1.1 Time-stamping protocol and time-stamp token profiles

	Security Requirements for trust service providers issuing electronic time-stamps

Regarding the certificate policies to be applied by 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 the 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 the eIDAS Regulation.

  QCP-n-qscd Certificate Policy for EU qualified certificates issued to natural persons with private keys 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 the 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 the eIDAS Regulation.

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

articles 36 and 37 of the eIDAS Regulation.

QCP-l-qscd	Certificate Policy for EU qualified certificates issued to legal persons with private keys related to the certified public key in a Qualified Electronic Signature Creation Device (hereinafter, QSCD). Includes all the QCP-l policy requirements (including all the NCP+ policy requirements), plus additional provisions suited to support EU qualified certificates issuance and management as specified in the 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 (27) of the 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 by IETF RFC 3647.

Regarding the Certification Authority AC CAMERFIRMA PERÚ CERTIFICADOS - 2016, these practices are aligned with Law No. 27269 *Ley de Firmas y Certificados Digitales*, its Regulations approved by *Decreto Supremo* No. 052-2008-PCM and the Guidelines for Certification Entities Accreditation published by the Competent Administrative Authority, the *Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual* (hereinafter, INDECOPI). As a Certification Entity, Camerfirma Perú, offers services for the issuance, revocation, and status information of digital certificates, using Camerfirma's technical and operational infrastructure, which fulfils the qualification regulatory framework defined by eIDAS Regulation and is verified annually by authorized auditors.

In addition, Camerfirma Perú offers the following services accredited by INDECOPI and therefore recognized in the *Infraestructura Oficial de Firma Electrónica* (IOFE):

- Registration or Entity verification.
- Time Stamping Value Added Service.
- Digital Intermediation added Value Service.
- Digital Signature Software.

If any provision of these practices does not apply to CA Perú, it will be expressly indicated (Does not apply to Camerfirma Perú), and in case of specific requirements of the Peruvian legal framework and only applicable to Camerfirma Perú, it will be expressly indicated (Applies only to Camerfirma Perú).

This CPS is compliant with the Certification Policies for the different certificates that Camerfirma issues, which are described in section 1.3.1.1 of this CPS. In the event of any conflict between both documents, the provisions of this document shall prevail.

1.2 DOCUMENT NAME AND IDENTIFICATION

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

1.3 COMMUNITY AND SCOPE OF APPLICATION

1.3.1 CERTIFICATION AUTHORITIES

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 checking and storing 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 organizing 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 has been specified in the Basic Constraints (pathLenConstraint) extension of the CA's certificate.

The following section describes the CAs hierarchies that Camerfirma manages as the owner (either directly or through subsidiaries) under this CPS. In the case of Intermediate CA owned by another organization, this CPS will refer to 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 hierarchies:

- Chambers of Commerce Root.
- Global Chambersign Root.

1.3.1.1 *CHAMBERS OF COMMERCE ROOT HIERARCHIES*

"CHAMBERS OF COMMERCE ROOT" IN ITS DIFFERENT VERSIONS IS THE PROPERTY OF AC CAMERFIRMA SA AS INDICATED IN THE FIELD ORGANIZATION OF THE ATTRIBUTE DN OF THE CORRESPONDING ROOT CERTIFICATE.

CHAMBERS OF COMMERCE ROOT SHA-256 fingerprint
0C:25:8A:12:A5:67:4A:EF:25:F2:8B:A7:DC:FA:EC:EE:A3:48:E5:41:E6:F5:CC:4E:E6:3B:71:B3:61:60:6A:C3
CHAMBERS OF COMMERCE ROOT SHA-1 fingerprint
6E:3A:55:A4:19:0C:19:5C:93:84:3C:C0:DB:72:2E:31:30:61:F0:B1
Chambers of Commerce Root - 2008 SHA-256 fingerprint
06:3E:4A:FA:C4:91:DF:D3:32:F3:08:9B:85:42:E9:46:17:D8:93:D7:FE:94:4E:10:A7:93:7E:E2:9D:96:93:C0

Chambers of Commerce Root - 2008 SHA-1 fingerprint
78:6A:74:AC:76:AB:14:7F:9C:6A:30:50:BA:9E:A8:7E:FE:9A:CE:3C
CHAMBERS OF COMMERCE - 2016 SHA-256 fingerprint
04:F1:BE:C3:69:51:BC:14:54:A9:04:CE:32:89:0C:5D:A3:CD:E1:35:6B:79:00:F6:E6:2D:FA:20:41:EB:AD:51
CHAMBERS OF COMMERCE - 2016 SHA-1 fingerprint
2D:E1:6A:56:77:BA:CA:39:E1:D6:8C:30:DC:B1:4A:BE:22:A6:17:9B

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

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

Within these hierarchies, different types of end-entity certificates are issued that may have been generated on QSCD devices and others on Non-QSCD devices.

For certificates issued on QSCD devices the keys are generated in:

- QSCD SmartCard/Token:
    - Qualified cryptographic smartcards.
    - Qualified cryptographic tokens.
- QSCD Cloud:
    - Centralized qualified cloud platform managed by Camerfirma.

And for certificates issued on Non-QSCD devices the keys are generated in:

- Non-QSCD:
    - PKCS #12.
    - Centralized non-qualified cloud platform managed by Camerfirma.
    - External device not managed by Camerfirma.
    - Non-qualified cryptographic smartcards or tokens.

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

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

is:

CHAMBERS OF COMMERCE ROOT – 2016	
AC CAMERFIRMA FOR NATURAL PERSONS - 2016	
1.3.6.1.4.1.17326.10.16.1.1.1 0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd]	Qualified Citizen Certificate - QCP-n-qscd in QSCD SmartCard/Token
1.3.6.1.4.1.17326.10.16.1.1.1 0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd] 1.3.6.1.4.1.17326.99.18.1	Qualified Citizen Certificate - QCP-n-qscd in QSCD Cloud
1.3.6.1.4.1.17326.10.16.1.1.2 0.4.0.194112.1.0 [ETSI EN 319 411 2 - QCP-n]	Qualified Citizen Certificate - QCP-n in Non-QSCD
1.3.6.1.4.1.17326.10.16.1.2.1 0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd]	Qualified Corporate Certificate - QCP-n-qscd in QSCD SmartCard/Token Qualified Corporate Certificate for Self-employed - QCP-n-qscd in QSCD SmartCard/Token Qualified Corporate Certificate for Chartered Self-employed – QCP-n-qscd in QSCD SmartCard/Token
1.3.6.1.4.1.17326.10.16.1.2.1 0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd] 1.3.6.1.4.1.17326.99.18.1	Qualified Corporate Certificate - QCP-n-qscd in QSCD Cloud Qualified Corporate Certificate for Self-employed - QCP-n-qscd in QSCD Cloud Qualified Corporate Certificate for Chartered Self-employed – QCP-n-qscd in QSCD Cloud
1.3.6.1.4.1.17326.10.16.1.2.2 0.4.0.194112.1.0 [ETSI EN 319 411 2 - QCP-n]	Qualified Corporate Certificate - QCP-n in Non-QSCD Qualified Corporate Certificate for Self-employed - QCP-n in Non-QSCD Qualified Corporate Certificate for Chartered Self-employed – QCP-n in Non-QSCD

1.3.6.1.4.1.17326.10.16.1.3.1.1 2.16.724.1.3.5.8 [national regulation] 0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd]	Qualified Certificate for a Representative of a Legal Entity with general powers of representation – QCP-n-qscd in QSCD SmartCard/Token
1.3.6.1.4.1.17326.10.16.1.3.1.1 2.16.724.1.3.5.8 [national regulation] 0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd] 1.3.6.1.4.1.17326.99.18.1	Qualified Certificate for a Representative of a Legal Entity with general powers of representation – QCP-n-qscd in QSCD Cloud
1.3.6.1.4.1.17326.10.16.1.3.1.2 2.16.724.1.3.5.8 [national regulation] 0.4.0.194112.1.0 [ETSI EN 319 411 2 - QCP-n]	Qualified Certificate for a Representative of a Legal Entity with general powers of representation – QCP-n in Non-QSCD
1.3.6.1.4.1.17326.10.16.1.3.1.1 2.16.724.1.3.5.9 [national regulation] 0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd]	Qualified Certificate for a Representative of a Non-Legal Entity with general powers of representation – QCP-n-qscd in QSCD SmartCard/Token
1.3.6.1.4.1.17326.10.16.1.3.1.1 2.16.724.1.3.5.9 [national regulation] 0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd] 1.3.6.1.4.1.17326.99.18.1	Qualified Certificate for a Representative of a Non-Legal Entity with general powers of representation – QCP-n-qscd in QSCD Cloud
1.3.6.1.4.1.17326.10.16.1.3.1.2 2.16.724.1.3.5.9 [national regulation] 0.4.0.194112.1.0 [ETSI EN 319 411 2 - QCP-n]	Qualified Certificate for a Representative of a Non-Legal Entity with general powers of representation – QCP-n in Non-QSCD
1.3.6.1.4.1.17326.10.16.1.3.2.1 2.16.724.1.3.5.8 [national regulation] 0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd]	Qualified Certificate for a Voluntary Representative of a Legal Entity before the Public Administrations - QCP-n-qscd in QSCD SmartCard/Token
1.3.6.1.4.1.17326.10.16.1.3.2.1 2.16.724.1.3.5.8 [national regulation] 0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd] 1.3.6.1.4.1.17326.99.18.1	Qualified Certificate for a Voluntary Representative of a Legal Entity before the Public Administrations - QCP-n-qscd in QSCD Cloud

1.3.6.1.4.1.17326.10.16.1.3.2.2 2.16.724.1.3.5.8 [national regulation] 0.4.0.194112.1.0 [ETSI EN 319 411 2 - QCP-n]	Qualified Certificate for a Voluntary Representative of a Legal Entity before the Public Administrations - QCP-n in Non-QSCD
1.3.6.1.4.1.17326.10.16.1.3.2.1 2.16.724.1.3.5.9 [national regulation] 0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd]	Qualified Certificate for a Voluntary Representative of a Non-Legal Entity before the Public Administrations - QCP-n-qscd in QSCD SmartCard/Token
1.3.6.1.4.1.17326.10.16.1.3.2.1 2.16.724.1.3.5.9 [national regulation] 0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd] 1.3.6.1.4.1.17326.99.18.1	Qualified Certificate for a Voluntary Representative of a Non-Legal Entity before the Public Administrations - QCP-n-qscd in QSCD Cloud
1.3.6.1.4.1.17326.10.16.1.3.2.2 2.16.724.1.3.5.9 [national regulation] 0.4.0.194112.1.0 [ETSI EN 319 411 2 - QCP-n]	Qualified Certificate for a Voluntary Representative of a Non-Legal Entity before the Public Administrations - QCP-n in Non-QSCD
1.3.6.1.4.1.17326.10.16.1.3.3.1 0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd]	Qualified Certificate for Special Representative of a Legal Entity - QCP-n-qscd in QSCD SmartCard/Token
1.3.6.1.4.1.17326.10.16.1.3.3.1 0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd] 1.3.6.1.4.1.17326.99.18.1	Qualified Certificate for Special Representative of a Legal Entity - QCP-n-qscd in QSCD Cloud
1.3.6.1.4.1.17326.10.16.1.3.3.2 0.4.0.194112.1.0 [ETSI EN 319 411 2 - QCP-n]	Qualified Certificate for Special Representative of a Legal Entity - QCP-n-qscd in QCP-n in Non-QSCD
1.3.6.1.4.1.17326.10.16.1.3.3.1 0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd]	Qualified Certificate for Special Representative of a Non-Legal Entity - QCP-n-qscd in QSCD SmartCard/Token
1.3.6.1.4.1.17326.10.16.1.3.3.1 0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd] 1.3.6.1.4.1.17326.99.18.1	Qualified Certificate for Special Representative of a Non-Legal Entity - QCP-n-qscd in QSCD Cloud

1.3.6.1.4.1.17326.10.16.1.3.3.2 0.4.0.194112.1.0 [ETSI EN 319 411 2 - QCP-n]	Qualified Certificate for Special Representative of a Non-Legal Entity - QCP-n in Non-QSCD
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.1 2.16.724.1.3.5.7.1 [Public administration high-level public employee] 0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd]	Qualified Certificate of Signature for Public Employee - QSCD SmartCard/Token. High Level.
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.1 2.16.724.1.3.5.7.1 [Public administration high-level public employee] 0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd] 1.3.6.1.4.1.17326.99.18.1	Qualified Certificate of Signature for Public Employee - QSCD Cloud. High Level.
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.2 2.16.724.1.3.5.7.1 [Public administration high-level public employee] 0.4.0.2042.1.2 [ETSI EN 319 411 1 - NCP+]	Qualified Certificate of Authentication for Public Employee - QSCD SmartCard/Token. High Level.
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.2 2.16.724.1.3.5.7.1 [Public administration high-level public employee] 0.4.0.2042.1.2 [ETSI EN 319 411 1 - NCP+] 1.3.6.1.4.1.17326.99.18.1	Qualified Certificate of Authentication for Public Employee - QSCD Cloud. High Level.
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.3 2.16.724.1.3.5.7.1 [Public administration high-level public employee]	Qualified Certificate of Encipherment for Public Employee - QSCD SmartCard/Token. High Level.
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.3 2.16.724.1.3.5.7.1 [Public administration high-level public employee] 1.3.6.1.4.1.17326.99.18.1	Qualified Certificate of Encipherment for Public Employee - QSCD Cloud. High Level.
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.4 2.16.724.1.3.5.7.2 [Public administration medium-level public employee] 0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd]	Qualified Certificate for Public Employee - QSCD SmartCard/Token. Medium Level.
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.4	Qualified Certificate for Public

2.16.724.1.3.5.7.2 [Public administration medium-level public employee] 0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd] 1.3.6.1.4.1.17326.99.18.1	Employee - QSCD Cloud. Medium Level.
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.4 2.16.724.1.3.5.7.2 [Public administration medium-level public employee] 0.4.0.194112.1.0 [ETSI EN 319 411 2 – QCP-n]	Qualified Certificate for Public Employee - Non-QSCD. Medium Level.
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.1 2.16.724.1.3.5.4.1 [Public administration high-level public employee] 0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd]	Qualified Certificate of Signature for Public Employee under a pseudonym - QSCD SmartCard/Token. High Level.
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.1 2.16.724.1.3.5.4.1 [Public administration high-level public employee] 0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd] 1.3.6.1.4.1.17326.99.18.1	Qualified Certificate of Signature for Public Employee under a pseudonym - QSCD Cloud. High Level.
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.2 2.16.724.1.3.5.4.1 [Public administration high-level public employee] 0.4.0.2042.1.2 [ETSI EN 319 411 1 - NCP+]	Qualified Certificate of Authentication for Public Employee under a pseudonym - QSCD SmartCard/Token. High Level.
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.2 2.16.724.1.3.5.4.1 [Public administration high-level public employee] 0.4.0.2042.1.2 [ETSI EN 319 411 1 - NCP+] 1.3.6.1.4.1.17326.99.18.1	Qualified Certificate of Authentication for Public Employee under a pseudonym - QSCD Cloud. High Level.
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.3 2.16.724.1.3.5.4.1 [Public administration high-level public employee]	Qualified Certificate of Encipherment for Public Employee under a pseudonym - QSCD SmartCard/Token. High Level.
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.3 2.16.724.1.3.5.4.1 [Public administration high-level public employee] 1.3.6.1.4.1.17326.99.18.1	Qualified Certificate of Encipherment for Public Employee under a pseudonym - QSCD Cloud. High Level.

1.3.6.1.4.1.17326.10.16.1.5.1.3.4.4 2.16.724.1.3.5.4.2 [Public administration medium-level public employee] 0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd]	Qualified Certificate for Public Employee under a pseudonym - QSCD SmartCard/Token. Medium Level.
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.4 2.16.724.1.3.5.4.2 [Public administration medium-level public employee] 0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd] 1.3.6.1.4.1.17326.99.18.1	Qualified Certificate for Public Employee under a pseudonym - QSCD Cloud. Medium Level.
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.4 2.16.724.1.3.5.4.2 [Public administration medium-level public employee] 0.4.0.194112.1.0 [ETSI EN 319 411 2 - QCP-n]	Qualified Certificate for Public Employee under a pseudonym - Non-QSCD. Medium Level.
AC CAMERFIRMA FOR LEGAL PERSONS - 2016	
1.3.6.1.4.1.17326.10.16.2.1.1 0.4.0.194112.1.3 [ETSI EN 319 411 2 - QCP-l-qscd]	Qualified Digital Seal Certificate - QSCD SmartCard/Token
1.3.6.1.4.1.17326.10.16.2.1.2 0.4.0.194112.1.1 [ETSI EN 319 411 2 - QCP-l]	Qualified Digital Seal Certificate - Non-QSCD
1.3.6.1.4.1.17326.10.16.2.3.2 0.4.0.2042.1.3 [ETSI EN 319 411 1 - LCP]	Digital Seal Certificate - Non-QSCD
1.3.6.1.4.1.17326.10.16.2.2.1.3.3.1 0.4.0.194112.1.3 [ETSI EN 319 411 2 - QCP-l-qscd] 2.16.724.1.3.5.6.1 [Electronic Seal for Public Administrations High Level]	Qualified Digital Seal Certificate for Public Administrations - QSCD SmartCard/Token. High Level.
1.3.6.1.4.1.17326.10.16.2.2.1.4.3.1 0.4.0.194112.1.3 [ETSI EN 319 411 2 - QCP-l-qscd] 2.16.724.1.3.5.6.2 [Electronic Seal for Public Administrations Medium Level]	Qualified Digital Seal Certificate for Public Administrations - QSCD SmartCard/Token. Medium Level.
1.3.6.1.4.1.17326.10.16.2.2.1.4.3.1 0.4.0.194112.1.1 [ETSI EN 319 411 2 - QCP-l] 2.16.724.1.3.5.6.2 [Medium]	Qualified Digital Seal Certificate for Public Administrations - Non-QSCD. Medium Level.
AC CAMERFIRMA TSA – 2016	

1.3.6.1.4.1.17326.10.16.5.1.1 0.4.0.194112.1.3 [ETSI EN 319 411 2 - QCP-l-qscd]	Qualified TSU Certificate - QSCD
IVSIGN CA Property of IVNOSYS SOLUCIONES, S.L.U. and it is governed by its CPS	
CHAMBERS OF COMMERCE ROOT – 2008	
AC CAMERFIRMA AAPP II – 2014	
1.3.6.1.4.1.17326.1.3.3.1	Recognized certificate of the electronic seal of Administration, body or entity of public law, high-level
1.3.6.1.4.1.17326.1.3.3.2	Recognized certificate of the electronic seal of Administration, body or entity of public law, medium-level
1.3.6.1.4.1.17326.1.3.4.1	Recognized public employee certificate, high-level, signature
1.3.6.1.4.1.17326.1.3.4.2	Recognized public employee certificate, high-level, authentication
1.3.6.1.4.1.17326.1.3.4.3	Recognized public employee certificate, high-level, encryption
1.3.6.1.4.1.17326.1.3.4.4	Recognized public employee certificate, medium-level
AC CAMERFIRMA CORPORATE SERVER II – 2015	
1.3.6.1.4.1.17326.10.11.3.1.1	Enterprise Electronic Seal Certificate Software - keys generated by the TSP
1.3.6.1.4.1.17326.10.11.3.1.2	Enterprise Electronic Seal Certificate Software - keys generated by the user
Camerfirma Codesign II – 2014	
Camerfirma TSA – 2013 This CA has no active certificates and does not issue new certificates.	
Camerfirma TSA II – 2014	

1.3.6.1.4.1.17326.10.13.1.3	TSU Certificate
CHAMBERS OF COMMERCE ROOT	
AC Camerfirma Express Corporate Server This CA has no active certificates and does not issue new certificates.	
AC CAMERFIRMA CERTIFICADOS CAMERALES	
1.3.6.1.4.1.17326.10.9.2.1.1	AC Camerfirma Certificados Camerales - Natural persons with a business relationship with an Entity – NCP
1.3.6.1.4.1.17326.10.9.2.1.2	AC Camerfirma Certificados Camerales - Natural persons with a business relationship with an Entity – NCP
1.3.6.1.4.1.17326.10.9.2.2.2	AC Camerfirma Certificados Camerales - Natural persons with a business relationship with an Entity – NCP SSCD
1.3.6.1.4.1.17326.10.16.1.3.2.2 2.16.724.1.3.5.8 [national regulation] 0.4.0.194112.1.0 [ETSI EN 319 411 2 - QCP-n]	Qualified Certificate of Voluntary Representative of an Entity with Legal Personality before the Public Administrations - QCP-n in Non-QSCD

1.3.1.1.1 AC CAMERFIRMA FOR LEGAL PERSONS. (CERTIFICADOS PARA PERSONAS JURÍDICAS)

1.3.1.1.1.1 QUALIFIED DIGITAL SEAL CERTIFICATE – QCP-L, QCP-L-QSCD

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

1.3.1.1.1.2 DIGITAL SEAL CERTIFICATE – LCP

This certificate is issued to a legal entity whose applicant must have representation or authorization

from the entity included in the certificate. This certificate can be associated with a key activated by a machine or application. Common transactions can be carried out automatically and without requiring intervention. The keys associated with the use of a digital seal certificate provide integrity and authenticity to the documents and transactions to which they apply. It can also be used as a client machine identification element in secure TLS communication protocols. The keys will be generated and stored in software support.

1.3.1.1.1.3 PUBLIC ADMINISTRATIONS DIGITAL SEAL CERTIFICATE. QCP-L, QCP-L-QSCD

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

1.3.1.1.2 AC CAMERFIRMA TSA (TIME STAMPING CERTIFICATES)

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

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

TSU qualified certificates have a maximum duration of five years by default.

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

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

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

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

is given.

The TSU certificate policies are:

1.3.1.1.2.1 QUALIFIED TSU CERTIFICATE IN QSCD

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

1.3.1.1.3 AC CAMERFIRMA FOR NATURAL PERSONS. (CERTIFICATES FOR NATURAL PERSONS) Y AC CAMERFIRMA CERTIFICADOS CAMERALES (CERTIFICATES FOR AUTHORIZED REPRESENTATIVES AND AC CAMERFIRMA CERTIFICADOS CAMERALES - NATURAL PERSONS WITH A BUSINESS RELATIONSHIP WITH AN ENTITY)

These are multi-policy Certification Authorities, which issue qualified and non-qualified certificates to natural persons within the territory of the European Union, the functionalities of which are described below.

The qualified certificates issued under these Certification Authorities that are issued in qualified devices incorporate a policy OID of type 1.3.6.1.4.1.17326.x.x.x.x.x.1.

The qualified certificates issued under these Certification Authorities that are issued on non-qualified devices incorporate a policy OID of type 1.3.6.1.1.4.1.17326.x.x.x.x.x.2.

The final certificates are intended for:

1.3.1.1.3.1 QUALIFIED CORPORATE CERTIFICATE OR QUALIFIED CORPORATE CERTIFICATE FOR SELF-EMPLOYED

1.3.1.1.3.1.1 Qualified Corporate Certificate - QCP-n-qscd in QSCD SmartCard/Token, QCP-n-qscd in QSCD Cloud, and QCP-n in Non-QSCD

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

1.3.1.1.3.1.2 Qualified Corporate Certificate for Self-employed - QCP-n-qscd in QSCD SmartCard/Token, QCP-n-qscd in QSCD Cloud or QCP-n in Non-QSCD

Determines the self-employed status of the natural person (holder of the certificate), informs of his/her economic activity, and, if applicable, of the registered trade name under which the self-employed person carries out his/her profession.

1.3.1.1.3.1.3 Qualified Corporate Certificate for Chartered Self-employed – QCP-n-qscd in QSCD SmartCard/Token, QCP-n-qscd in QSCD Cloud or QCP-n in Non-QSCD

Determines the self-employed status of the natural person (holder of the certificate), provides information on their professional activity, their status as a registered professional, and, if applicable, the registered trade name under which the self-employed person carries out their profession.

1.3.1.1.3.2 QUALIFIED REPRESENTATIVE CERTIFICATE

1.3.1.1.3.2.1 Qualified Certificate for a Representative of a Legal Entity with general powers of representation – QCP-n-qscd in QSCD SmartCard/Token, QCP-n-qscd in QSCD Cloud or QCP-n in Non-QSCD

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

It is addressed to legal representatives of entities with legal personality such as Sole Administrator, Joint Administrator, Director-Delegate, etc., and voluntary General Power of Attorneys which include very broad powers of representation (similar to those of a legal representative) that allows them to act both in the field of relationships and procedures with Public Administrations and in the field of contracting of goods or services or concerning the ordinary business of the organization.

The 'Jointly and Severally' legal representatives or the 'Jointly and Severally' empowered person by a General Power of Attorneys who want to request this certificate must hold powers that include at least, the jointly and severally power to represent the Legal Person to carry out relationships and procedures with Public Administrations. In this regard, the Certificate Holder is in charge of using it by its Powers and the trust User Party to verify its content and scope.

1.3.1.1.3.2.2 Qualified Certificate for a Representative of a Non-Legal Entity with general powers of representation – QCP-n-qscd in QSCD SmartCard/Token, QCP-n-qscd in QSCD Cloud or QCP-n in Non-QSCD

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

It is addressed to legal representatives of Non-legal Entity such as Sole Administrator, Joint Administrator, manager, President of Property Owners, etc., and empowered person with General Power of Attorneys which include very broad powers of representation (similar to those of a legal representative) that allows them to act both in the field of relationships and procedures with Public Administrations and in the field of contracting of goods or services or concerning the ordinary

business of the organization.

The 'Jointly and Severally' legal representatives or the 'Jointly and Severally' empowered persons with General Power of Attorneys who want to request this certificate must hold powers that include at least, the jointly and severally power to represent the Non-legal Entity to carry out relationships and procedures with Public Administrations. In this regard, the Certificate Holder is in charge of using it by its Powers and the trusted User Party to verify its content and scope.

1.3.1.1.3.2.3 Qualified Certificate for a Voluntary Representative of a Legal Entity before the Public Administrations - QCP-n-qscd in QSCD SmartCard/Token, QCP-n-qscd in QSCD Cloud or QCP-n in Non-QSCD

Its purpose is to identify an individual and add the attribute (information) that such person may represent in an entity with legal status in its relations with the Public Administration (authentication and signature uses).

It is addressed to Legal Representatives, an empowered person with General Power of Attorneys or Specific Power of Attorneys which include at least one paragraph that enables them to request electronic certificates to perform on behalf of the entity with legal status, actions, and procedures with Public Administrations that require the use of the electronic signature or electronic certificate.

The 'Jointly and Severally' legal representatives or 'Jointly and Severally' empowered persons with General Power of Attorneys or Specific Power of Attorneys may request this certificate as long as their powers include at least the jointly and severally power to represent the Legal Person 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 this regard, the Certificate Holder is in charge of using it by its Powers and the trusted User Party to verify its content and scope.

1.3.1.1.3.2.4 Qualified Certificate for a Voluntary Representative of a Non-Legal Entity before the Public Administrations - QCP-n-qscd in QSCD SmartCard/Token, QCP-n-qscd in QSCD Cloud or QCP-n in Non-QSCD

Its purpose is to identify an individual and add the attribute (information) that such person may represent in an entity with legal status in its relations with the Public Administration (authentication and signature uses).

It is addressed to Legal Representatives, an empowered person with General Power of Attorneys or Specific Power of Attorneys which include at least one paragraph that enables 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 and Severally' legal representatives or 'Jointly and Severally' empowered persons with General Power of Attorneys or Specific Power of Attorneys may request 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 signed by all the jointly empowered persons in favor of one of them. In this regard, the Certificate Holder is in charge of using it by its Powers and the trusted User Party to verify its content and scope.

1.3.1.1.3.2.5 Qualified Certificate for Special Representative of a Legal Entity - QCP-n-qscd in QSCD SmartCard/Token, QCP-n-qscd in QCP-n-qscd in QSCD Cloud or QCP-n in Non-QSCD

This certificate identifies a natural person (Holder/Subject/Signatory) and determines as specific attributes, his/her capability to act on behalf of an entity with legal status only for certain powers or faculties framed in his/her function/department (signature uses for private documents in the ordinary commercial activity of the represented entity).

This certificate is not valid for authentication or signature uses on behalf of the entity with legal status 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 for 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 by its Powers and the Relying Party to verify its content and scope.

1.3.1.1.3.2.6 Qualified Certificate for Special Representative of a Non-Legal Entity - QCP-n-qscd in QSCD SmartCard/Token, QCP-n-qscd in QSCD Cloud or QCP-n in Non-QSCD

This certificate identifies a natural person (Holder/Subject/Signatory) and determines as specific attributes, his/her capability to act on behalf of an entity with non-legal status only for certain powers or faculties framed in his/her function/department (signatures uses for private documents in the ordinary commercial activity of the represented entity).

This certificate is not recommended valid for authentication or signature uses on behalf of the entity with non-legal status 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 for 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 by its Powers and the Relying Party to verify its content and scope.

1.3.1.1.4 PUBLIC EMPLOYEE CERTIFICATES – QCP-N, QCP-N-QSCD, NCP+

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

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

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

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

1.3.1.1.5 AC CAMERFIRMA CERTIFICADOS CAMERALES - NATURAL PERSONS WITH A BUSINESS RELATIONSHIP WITH AN ENTITY - NCP

This Certification Authority issues non-qualified certificates to natural persons within the territory of the European Union.

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

1.3.1.1.6 NATURAL PERSONS WITH NO BUSINESS RELATIONSHIP WITH AN ENTITY

1.3.1.1.6.1 QUALIFIED CITIZEN CERTIFICATE - QCP-N-QSCD IN QSCD SMARTCARD/TOKEN, QSCD CLOUD, OR QCP-N IN NON-QSCD

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

1.3.1.1.7 EXPRESS CORPORATE SERVER

This is an intermediate CA that issues digital certificates whose titular are machines or applications. This CA issues this policy:

1.3.1.1.7.1 ENTERPRISE ELECTRONIC SEAL CERTIFICATE

This certificate is associated with a key protected by a machine or application. The operations commonly performed are automatic and unassisted. The action of the keys associated with the electronic seal certificate gives integrity and authenticity to the documents and transactions to which it is applied. It can also be used as a machine client identification element in SSL/TLS or HTTPS secure communication protocols, as well as information encryption.

1.3.1.1.8 CAMERFIRMA CODESIGN II - 2014

Intermediate CA called "Camerfirma CodeSign" issues certificates for code signing. The certificates for code signing allow as the name suggests, developers to apply an electronic signature on the code they develop: ActiveX, java applets, macros for Microsoft Office, etc. thus establishing, in this way, on said code, guarantees of integrity and authenticity.

1.3.1.1.9 IVSIGN CA

IVSIGN CA is an intermediate CA owned by the company IVNOSYS SOLUCIONES, S.L.U. which is governed by its CPS that must comply with at least the provisions of this CPS of the CA Root to which it belongs. In case of discrepancy, the provisions of the CPS of the CA Root will prevail. The purpose of this intermediate CA will be to issue subordinate CA certificates with a scope within the territory of the European Union.

1.3.1.2 GLOBAL CHAMBERSIGN ROOT HIERARCHIES

"GLOBAL CHAMBERSIGN ROOT" IN ITS DIFFERENT VERSIONS IS THE PROPERTY OF AC CAMERFIRMA SA AS INDICATED IN THE FIELD ORGANIZATION OF THE ATTRIBUTE CN OF THE CORRESPONDING ROOT CERTIFICATE.

GLOBAL CHAMBERSIGN ROOT - 2016 SHA-256 fingerprint
C1:D8:0C:E4:74:A5:11:28:B7:7E:79:4A:98:AA:2D:62:A0:22:5D:A3:F4:19:E5:C7:ED:73:DF:BF:66:0E:71:09
GLOBAL CHAMBERSIGN ROOT - 2016 SHA-1 fingerprint
11:39:A4:9E:84:84:AA:F2:D9:0D:98:5E:C4:74:1A:65:DD:5D:94:E2
Global Chambersign Root – 2008 - SHA-256 fingerprint
13:63:35:43:93:34:A7:69:80:16:A0:D3:24:DE:72:28:4E:07:9D:7B:52:20:BB:8F:BD:74:78:16:EE:BE:BA:CA
Global Chambersign Root – 2008 - SHA-1 fingerprint
4A:BD:EE:EC:95:0D:35:9C:89:AE:C7:52:A1:2C:5B:29:F6:D6:AA:0C
Global Chambersign Root - SHA-256 fingerprint
EF:3C:B4:17:FC:8E:BF:6F:97:87:6C:9E:4E:CE:39:DE:1E:A5:FE:64:91:41:D1:02:8B:7D:11:C0:B2:29:8C:ED
Global Chambersign Root - SHA-1 fingerprint

33:9B:6B:14:50:24:9B:55:7A:01:87:72:84:D9:E0:2F:C3:D2:D8:E9
GLOBAL CHAMBERSIGN ROOT - 2016 SHA-256 fingerprint
C1:D8:0C:E4:74:A5:11:28:B7:7E:79:4A:98:AA:2D:62:A0:22:5D:A3:F4:19:E5:C7:ED:73:DF:BF:66:0E:71:09
GLOBAL CHAMBERSIGN ROOT - 2016 SHA-1 fingerprint
11:39:A4:9E:84:84:AA:F2:D9:0D:98:5E:C4:74:1A:65:DD:5D:94:E2

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

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

Within the framework of this hierarchy, different intermediate certification authorities correspond to the global, national, sector, and corporate frameworks and that may be well owned by Camerfirma, or by third organizations.

GLOBAL CHAMBERSIGN ROOT – 2016	
AC CAMERFIRMA COLOMBIA – 2016 (SUBCA DE GLOBAL CHAMBERSIGN ROOT – 2016)	
CAMERFIRMA COLOMBIA SAS CERTIFICADOS – 001 (SUBCA DE AC CAMERFIRMA COLOMBIA – 2016) Property of CAMERFIRMA COLOMBIA SAS and it is governed by its CPS	
CAMERFIRMA COLOMBIA SAS CERTIFICADOS – 002 (SUBCA DE AC CAMERFIRMA COLOMBIA – 2016) Property of CAMERFIRMA COLOMBIA SAS and it is governed by its CPS	
AC CAMERFIRMA PERÚ – 2016 (SUBCA DE GLOBAL CHAMBERSIGN ROOT – 2016)	
AC CAMERFIRMA PERÚ CERTIFICADOS – 2016 (SUBCA DE AC CAMERFIRMA PERÚ – 2016)	
1.3.6.1.4.1.17326.30.16.0.1	Legal Entity Certificate - Entity Membership Attribute
1.3.6.1.4.1.17326.30.16.0.2	Legal Entity Certificate - Entity Membership Attribute SSCD

1.3.6.1.4.1.17326.30.16.0.3	Legal Entity Certificate - Entity Membership Attribute Cloud
1.3.6.1.4.1.17326.30.16.10.1	Legal Entity Certificate - Representative Attribute
1.3.6.1.4.1.17326.30.16.10.2	Legal Entity Certificate - Representative Attribute SSCD
1.3.6.1.4.1.17326.30.16.20.1	Legal Entity Certificate
1.3.6.1.4.1.17326.30.16.20.2	Legal Entity Certificate SSCD
1.3.6.1.4.1.17326.30.16.30.1	Legal Entity Certificate - Electronic Invoice Attribute
1.3.6.1.4.1.17326.30.16.30.2	Legal Entity Certificate - Electronic Invoice Attribute SSCD
1.3.6.1.4.1.17326.30.16.40.1	Natural Person Certificate
1.3.6.1.4.1.17326.30.16.40.2	Natural Person Certificate SSCD
1.3.6.1.4.1.17326.30.16.40.3	Natural Person Certificate Cloud
1.3.6.1.4.1.17326.30.16.50.1	Companies Electronic Seal Certificate for an automatized agent
1.3.6.1.4.1.17326.30.16.50.1	Companies Electronic Seal Certificate in Panama
1.3.6.1.4.1.17326.30.16.50.2	Companies Electronic Seal Certificate for automatized agent SSCD
1.3.6.1.4.1.17326.30.16.60.1	Legal Person Certificate - Registered Professional Attribute
1.3.6.1.4.1.17326.30.16.60.2	Legal Person Certificate - Registered Professional Attribute SSCD
1.3.6.1.4.1.17326.30.16.60.3	Legal Person Certificate - Registered Professional Attribute Cloud
GLOBAL CHAMBERSIGN ROOT – 2008	
AC CAMERFIRMA – 2009 This CA only issues CA certificates	
Entitat de Certificació de l'Administració Pública Andorrana-19 Owned by the M.I. Govern d'Andorra and governed by its CPS	
MULTICERT SSL Certification Authority 001 Owned by MULTICERT - Serviços de Certificação Eletrónica S.A. and governed by its own CPS	
GLOBAL CORPORATE SERVER This CA only issues CA certificates	
InfoCert Organization Validation CA 3 (SUBCA DE GLOBAL CORPORATE SERVER) Owned by InfoCert S.p.A. and governed by its CPS	
InfoCert Organization Validation 2019 CA 3 (SUBCA DE GLOBAL CORPORATE SERVER) Owned by InfoCert S.p.A. and governed by its CPS	

AC Camerfirma Portugal – 2015 This CA only issues CA certificates	
DigitalSign Primary CA (SUBCA DE AC Camerfirma Portugal – 2015) Owned by DigitalSign Certificadora Digital and governed by its CPS	
DigitalSign CA (SUBCA DE DigitalSign Primary CA) Owned by DigitalSign Certificadora Digital and governed by its CPS	
DigitalSign TSA CA (SUBCA DE DigitalSign Primary CA) Owned by DigitalSign Certificadora Digital and governed by its CPS	
Global Chambersign Root	
AC Camerfirma This CA only issues CA certificates	
RACER (SUBCA DE AC Camerfirma)	
1.3.6.1.4.1.17326.10.8.6.1.1	AC Camerfirma Citizen Certificate
1.3.6.1.4.1.17326.10.8.6.2.1	AC Camerfirma Citizen Certificate - Hardware - TSP generated keys
1.3.6.1.4.1.17326.10.8.6.2.2	AC Camerfirma Citizen Certificate - Hardware – user-generated keys

1.3.1.2.1 AC CAMERFIRMA COLOMBIA

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

1.3.1.2.1.1 CAMERFIRMA COLOMBIA S.A.S. CERTIFICADOS – 001

CAMERFIRMA COLOMBIA S.A.S. CERTIFICADOS – 001 is an intermediate CA owned by the Colombian national company CAMERFIRMA COLOMBIA S.A.S. (not mainly owned by AC Camerfirma SA) which is governed by its own CPS that must comply with at least the provisions of this CPS of the Root CA to which it belongs. In case of discrepancy, the provisions of the CPS of the Root CA will prevail.

1.3.1.2.1.2 CAMERFIRMA COLOMBIA S.A.S. CERTIFICADOS – 002

CAMERFIRMA COLOMBIA S.A.S. CERTIFICADOS – 002 is an intermediate CA owned by the Colombian national company CAMERFIRMA COLOMBIA S.A.S. (not mainly owned by AC Camerfirma SA) which is governed by its own CPS that must comply with at least the provisions of this CPS of the Root CA to which it belongs. In case of discrepancy, the provisions of the CPS of the Root CA will prevail.

1.3.1.2.2 AC CAMERFIRMA PERÚ

AC CAMERFIRMA PERÚ is an intermediate CA owned by CAMERFIRMA PERÚ S.A.C (mainly owned by AC Camerfirma SA) whose purpose is to issue Subordinate CA certificates within the geographic scope of the Republic of Perú and generally, in LATAM countries which can recognize its validity.

This intermediate CA has started its activity in August 2017 after receiving authorization from the Peruvian national supervisory body "INDECOPI". These Practices and other regulatory documents are published on the Camerfirma Perú website www.camerfirma.com.pe.

Regarding the roles of Holder, Subscriber, and Entity, the following descriptions of the different profiles issued by AC Camerfirma Perú Certificates - 2016 take into account the terminology used in the Peruvian legal framework applicable to digital signatures and certificates.

1.3.1.2.2.1 AC CAMERFIRMA PERU CERTIFICATES (CERTIFICATES FOR NATURAL AND LEGAL ENTITIES)

1.3.1.2.2.1.1 Legal Entity Certificate – Entity Membership Attribute (Certificates for legal persons)

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

In the INDECOPI Guidelines, the Entity is considered the Certificate Holder and the Natural Person the Subscriber of the certificate.

1.3.1.2.2.1.2 Legal Entity Certificate – Representative Attribute (Certificates for legal persons)

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

In the INDECOPI Guidelines, the Entity is considered the Certificate Holder and the Natural Person the Subscriber of the certificate.

1.3.1.2.2.1.3 Legal Entity Certificate (Certificates for legal entities)

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

1.3.1.2.2.1.4 Legal Entity Certificate - Electronic Invoice Attribute (Certificates for legal persons)

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

In the INDECOPI Guidelines, the Entity is considered the Certificate Holder and the Natural Person the Subscriber of the certificate.

1.3.1.2.2.1.5 Natural Person Certificate (Certificates for individuals)

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

1.3.1.2.2.1.6 Companies Electronic Seal Certificate for an automatized agent (Certificates for legal persons)

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

1.3.1.2.2.1.7 Companies Electronic Seal Certificate in Panama (Certificate for legal persons)

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

1.3.1.2.2.1.8 Legal Person Certificate - Registered Professional Attribute

It determines the relationship between a natural person and a Peruvian Professional Association (organization field of the certificate).

1.3.1.3 CAMERFIRMA INTERNAL MANAGEMENT HIERARCHY

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

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

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

1.3.1.4 ISSUING GENERAL TEST CERTIFICATES

Camerfirma issues certificates with a real hierarchy but with fictitious data to provide them to regulatory entities, inspection procedures, or new registration processes, as well as for application developers in the process of integration or evaluation for acceptance. Camerfirma includes the following information in the certificates so that the User Party can 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 the accreditation and evaluation process requires the issuance of a test certificate with real data, the process is completed after signing a confidentiality agreement with the entity responsible for approval or evaluation tasks. The data is specific to each customer, but before the entity name '[SOLO PRUEBAS]' or '[TEST ONLY]' always appears to identify at first glance that it is a test certificate without liability.

1.3.2 REGISTRATION AUTHORITY (RA)

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

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

- Chambers RA: Those managed directly or under the control of a Spanish Chamber of Commerce, Industry, and Navigation.
- Corporate RA: Managed by a public organization or a private entity for distributing certificates to its employees.
- Remote RA: A registration authority managed in a remote location that communicates with the platform through the Camerfirma STATUS® management platform integration layer.
- Entity Registry or RE for AC CAMERFIRMA PERÚ CERTIFICADOS – 2016.

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

- The Certification Authority.
- The Spanish Chambers of Commerce, Industry, and Navigation, or the entities appointed by them. The delegated entities can carry out the registration process.
- Spanish Company Registration Authorities (Company RA), as entities delegated by an RA, to which they are contractually associated, to make the complete records of Subjects/Signatories within a particular organization or demarcation. In general, the operators of these RA companies only manage the applications and certificates 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, and members of a professional body.
- Entities belonging to the Spanish public administrations.
- Other Spanish or international agents that have a contractual relationship with the CA and have passed the registration processes. They are obliged to pass the audits required in the corresponding Certification Policies. 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 requirements.
- The ER of Camerfirma Perú as long as it obtains the corresponding Accreditation from INDECOPI
- The external ERs that participate in the certificate issuance of the CA AC CAMERFIRMA PERÚ CERTIFICADOS – 2016, based on a contractual relationship with Camerfirma Perú that authorizes them to carry out the previous registration tasks once they obtain the official INDECOPI Accreditation.
- PVP. Point of Physical Verification that always depends on an RA. Its main mission is to provide evidence of the applicant's physical presence and deliver the documentation to the RA, which is validated with the applicable policy for processing the application for issuing the certificate. For these functions, the PVPs are not subject to training or controls.
- Sometimes, the PVPs' functions may be extended to compiling the documentation submitted, checking its suitability for the type of certificate requested, and delivery to the applicant in the case of the cryptographic card. Camerfirma has drafted a relationship-type document between the RA and the PVP.

- Given that they cannot register, they are contractually linked to an RA through a standard contract provided by Camerfirma. Based on the documentation provided by the PVP, the operator of the RA checks the documentation, and if applicable, gives course to the issuance of the certificate by the CA without having to make another face-to-face verification. The contract defines the functions delegated by the RA in the PVP.
- Subsidiary (only applicable for AC CAMERFIRMA PERU -2016): the RA (called "Registration Entities" or "RE" according to the nomenclature of the Official Electronic Signature Infrastructure of INDECOPI) may have branches that perform the same functions as the main RE in geographic areas far from the domicile of the RE. The Branches will be subject to the same controls and follow-up as the main RE and must assume the same obligations and responsibilities and submit to the audits and evaluations made to the RE by the competent supervisory body (INDECOPI).

  At the time of opening a Subsidiary, the ER must immediately inform INDECOPI and deliver a document specifying the location of the agency, as well as the names of those responsible for the registration processes, to allow the evaluation of said Subsidiary within the deadlines set by the administrative authority.

1.3.3 SUBJECT/HOLDER AND SIGNATORY/CREATOR OF THE SEAL

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

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

By Signatory/Creator of the seal we mean the one who creates the electronic signature or the electronic seal.

- When it's a physical person the Signatory is also Subject/Holder and can be:
  - A natural person with no attachment to an entity/organization.
  - A natural person representing an entity/organization with or without legal personality.
  - A natural person authorized to be identified as belonging to an entity/organization with or without legal personality and who is identified in association with the organization (O) field of the certificate.
- When it's a legal person, the Creator of the Seal coincides with the Subject/Holder of the certificate.

- When it's a device, the Signatory may be:
  - The natural person operating the device or application.
  - Any entity authorized to represent the legal entity.
  - A legal representative.

The Signatory/Creator of the Seal, as the Subject/Holder of the certificate, shall be directly responsible for the obligations associated with the use and management of the Seal.

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

(Applies only to Camerfirma Perú) According to the Peruvian legal framework of digital signatures and certificates, the Holder of the certificate can be the natural or legal person to whom a digital certificate is exclusively attributed. Within the IOFE of Perú, the responsibility for the legal effects generated by the use of a digital signature corresponds to the Holder. In the case of natural persons, they are Holders and Subscribers of the digital certificate. In the case of legal persons, they are Holders of the digital certificate.

1.3.4 RELAYING PARTIES

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

1.3.5 OTHER PARTICIPANTS

1.3.5.1 ACCREDITATION ENTITY OR SUPERVISORY BODY

The supervision authority is the corresponding management entity that accepts, accredits, and supervises the TSPs within a specific geographic area. The national supervisor body within the Spanish State is the *Ministerio de Asuntos Económicos y Transformación Digital*, which is the competent authority depending on the Spanish State member of the European Economic Space. In Perú, the Competent Administrative Authority is INDECOPI.

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

1.3.5.2 TRUSTED SERVICE PROVIDER (TSP)

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

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

The trusted services defined in the eIDAS Regulation include:

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

1.3.5.3 ENTITY/ORGANIZATION

The Entity is a public or private, individual or collective organization, recognized under the law, with which the natural person/certificate Holder maintains a certain relationship, as defined in the ORGANIZATION field (O) in each certificate. In the case of electronic seal certificates, the Entity is the Creator of the Seal/certificate Holder and is also defined in the (O) ORGANIZATION field of each certificate.

1.3.5.4 APPLICANT

Under this CPS, Applicant means the Subject/Holder when the Subject/Holder is a natural person, and the natural person who performs the application processing is the Subject/Holder when the Subject/Holder is a legal person and is responsible for the use of the certificate.

(Applies only to Camerfirma Perú) According to the Peruvian legal framework applicable to digital signatures and certificates, the Applicant is called a "Subscriber" and is the natural person responsible for the generation and use of the private key. He/she is linked in exclusive with an electronic document digitally signed using his/her private key. If the Holder of the digital certificate is a natural person, the responsibility of the subscriber will fall on him/her. If the Holder of a digital certificate is a legal person, the responsibility of the subscriber will fall on the legal representative appointed by this legal entity. If the certificate is oriented to be used by an automated agent, the attribution of subscriber responsibility, for such purposes, corresponds to the legal person which acts as the Holder of the certificate.

1.3.5.5 CERTIFICATE HOLDER/KEY HOLDER

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

For certificates issued to legal persons, without prejudice to the obligations of the Subject/Holder, this CPS holds the Applicant responsible, even if the application is made through a third party when the latter becomes aware of the existence of the certificate.

For component certificates, without prejudice to the obligations of the Subject/Holder, this CPS considers the physical person Applicant responsible, even if the application is made through a third party when the latter becomes aware of the existence of the certificate.

(Applies only to Camerfirma Perú) According to the Peruvian legal framework, the Responsible for the certificate will be the Subscriber as defined in section 1.3.5.4.

1.4 SCOPE OF APPLICATION AND CERTIFICATE USAGE

1.4.1 APPROPRIATE CERTIFICATE USES

Certificates issued under these policies are used for the following purposes:

- Certificate holder authentication.

  For natural person certificates.

  For legal person certificates such as Seals.

- Electronic, advanced, or qualified signature when used with qualified electronic signature creation devices.

  For electronic seals, advanced or qualified when used with qualified electronic seals creation devices.

- Asymmetric or mixed encryption without key recovery.

1.4.2 PROHIBITED AND UNAUTHORIZED CERTIFICATE USES

Camerfirma includes information on the limitation of use in the certificate, either in standardized 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.

Certificates are not designed, may not be used and their use or resale is not authorized as control

equipment for dangerous situations or for uses requiring fail-safe actions, such as the operation of nuclear facilities, navigation systems or aerial communication or weapon control systems, where an error could directly result in death, personal injury, or severe environmental damage.

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

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

(Applies only to Camerfirma Perú) In addition, uses not compliant with Peruvian regulations are not allowed.

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 are 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)

Telephone: +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 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 which is the legal department of Camerfirma.

Camerfirma publishes every new version of this document on its website https://policy.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

AWS	Amazon Web Services
CA	Certification Authority
CE	Certification Entity (Applies only to Camerfirma Perú)
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DES	Data Encryption Standard
DN	Distinguished Name. A distinguished name in the digital certificate
DSA	Digital Signature Algorithm. The signature's algorithm standard
EEA	European Economic Area
EU	European Union
FIPS	Federal Information Processing Standard
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ITU	International Telecommunications Union

LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PA	Policy Authority
CP	Certification Policy
PIN	Personal Identification Number
PKI	Public Key Infrastructure
QSCD	Qualified Signature Creation Device. The component used by the Subject/Signatory for the generation of electronic signatures, so that cryptographic operations are carried out within the device and its control is guaranteed solely by the Subject/Signatory.
RA	Registration Authority
RE	Registration Entity (Applies only to Camerfirma Perú)
RSA	Rivest-Shamir-Adleman. Type of encryption algorithm
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer. A protocol designed by Netscape has become standard on the Internet. It allows the transmission of encrypted information between a browser and a server.
TCP/IP	Transmission Control. Protocol/Internet Protocol. System of protocols, as defined in the IETF framework. The TCP protocol is used to split source information into packets and then recompile it on arrival. The IP protocol is responsible for correctly directing the information to the recipient.
TLS	Transport Layer Security. A secure communication protocol that replaces SSL.

1.6.2 DEFINITIONS

Activation data	Private data such as PINs or passwords are used for activating the private key.
Applicant	Within the context of this certification policy, the applicant may be the Subject/Certificate Holder itself or a natural person authorized or empowered to carry out certain procedures in the name and on behalf of the entity.
Certificate	A file that associates the public key with some data identifying the Subject/Signatory and signed by the CA.
Certification Authority	This is the entity responsible for issuing and managing digital certificates. It acts as the trusted third party between the Subject/Signatory and the User

	Party, associating a specific public key with a person. For this CPS, the name "Certification Authority" or "CA" will be applied both to the CAs of Camerfirma and the EC of Camerfirma Perú.
Certification Policy	A set of rules defining the applicability of a certificate in a community and/or in an application, with common security and usage requirements.
CPS	Defined as a set of practices adopted by a Certification Authority for issuing certificates in compliance with a specific certification policy.
CRL	A file containing a list of certificates that have been revoked for a certain period and which is signed by the CA.
Cross certification	The establishment of a trust relationship between two CAs, by exchanging certificates between the two under similar security levels.
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.
Registration Authority	The entity is responsible for managing applications and the identification and registration of certificates. For these CPS, the name "Registration Authority" or "RA" will be applied both to the RAs of Camerfirma and the ERs of Camerfirma Perú.
Remote Signature	A special qualified electronic signature or digital signature procedure is generated by an HSM that guarantees the sole control of the signatory's private keys and allows the creation of electronic signatures remotely.
Remote Seal	Special qualified electronic seal procedure generated by an HSM that guarantees the sole control of the private keys of the Seal Creator and allows the creation of electronic seals remotely.
OID	A unique numeric identifier registered under the ISO standardization and referring to a particular object or object class.
PKI	A set of hardware, software, and human resources elements and procedures, etc., that a system is made up of based on the creation and management of public key certificates.

Policy authority	A person or group of people responsible for all decisions relating to the creation, management, maintenance, and removal of certification and CPS policies.
Private key	A mathematical value known only to the Subject/Signatory and used for creating a digital signature or decrypting data. Also called signature creation data. The CA's private key is to be used for signing certificates and CRLs.
Public key	A publicly known mathematical value is used for verifying a digital signature or encrypting data. Also called signature verification data.
Subject/Creator of the seal	Within the context of this certification practice statement, the legal person creates an electronic seal.
Subject/Signatory	Within the context of this certification practices statement, the natural person whose public key is certified by the CA and who has a valid private key for generating digital signatures.
User Party	Within the context of this certification policy, the person who voluntarily trusts the digital certificate and uses it as a means for accrediting the authenticity and integrity of the signed document.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORY

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

For Perú: https://www.camerfirma.com.pe/validador-de-certificados/

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

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

For Perú: https://www.camerfirma.com.pe/normativa/

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

For Perú: https://www.camerfirma.com.pe/validador-de-certificados/

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

2.2 PUBLICATION OF CERTIFICATION INFORMATION

Camerfirma generally publishes the following information in its repository:

- An updated certificate directory indicating the certificates issued and whether they are valid or their application has been suspended or terminated. https://www.camerfirma.com/ayuda/utilidades/validacion-de-certificados/

  For Perú: https://www.camerfirma.com.pe/validador-de-certificados/

- The lists of revoked certificates and other information about the status of revoked certificates. https://www.camerfirma.com/ayuda/utilidades/validacion-de-certificados/

  For Perú: https://www.camerfirma.com.pe/validador-de-certificados/

- The general certification policy and, where appropriate, specific policies. https://www.camerfirma.com/practicas-de-certificacion-ac-camerfirma-cps-dpc/ - https://www.camerfirma.com/politicas-de-certificacion-ac-camerfirma.

  For Perú: https://www.camerfirma.com.pe/normativa/

- Certificate profiles and lists of revoked certificates can be asked at https://www.camerfirma.com/contacto-soporte/.

- The Certification Practices Statement and the corresponding PDS (PKI Disclosure Statement).

https://www.camerfirma.com/practicas-de-certificacion-ac-camerfirma-cps-dpc/

For Perú: https://www.camerfirma.com.pe/normativa/

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

Camerfirma shall not remove the previous version of the changed document, indicating that it has been replaced by the new version. However, any version can be requested through https://www.camerfirma.com/contacto-soporte/

External Subordinate CA certificates are published in a repository provided by Camerfirma, or if applicable, in its repository which, by contractual agreement, Camerfirma can access. However, any certificate can be requested through https://www.camerfirma.com/contacto-soporte/

2.2.1 CERTIFICATION POLICIES AND PRACTICES

These CPS and Policies are available to the public on the following website: https://www.camerfirma.com/practicas-de-certificacion-ac-camerfirma-cps-dpc/.

For Perú: https://www.camerfirma.com.pe/normativa/

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

2.2.2 TERMS AND CONDITIONS

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

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

2.2.3 DISTRIBUTION OF THE CERTIFICATES

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

https://www.camerfirma.com/ayuda/utilidades/validacion-de-certificados/.

The root keys in the Camerfirma hierarchies can be downloaded from:

https://www.camerfirma.com/ayuda/utilidades/descarga-de-claves-publicas/

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

2.3 PUBLICATION FREQUENCY

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

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

A new version of the CPS will be created at least once a year. Camerfirma immediately publishes it on its website https://policy.camerfirma.com. Any change to the Policies and the CPS, maintaining a version log.

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

2.4 ACCESS CONTROLS TO REPOSITORIES

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

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

Camerfirma uses reliable systems for the repository, so that:

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

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 TYPES OF NAMES

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

Profile records can be requested through Camerfirma customer support service on +34 911 36 91 05 or via the application https://www.camerfirma.com/contacto-soporte/.

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 of their full name and tax ID number.
- Legal entities: In certificates corresponding to legal entities, this identification is via their corporate name and tax identification.
- Components or devices: The final entity certificates describing components or devices incorporate an identifying name of the machine or service, in addition to the legal entity that owns the service in the organization field "O" of the "CN".
- The structure for Subordinate CA, TSU, TSA, and OCSP certificates includes at least:
    - A descriptive name that identifies the Certification Authority (CN)
    - The legal entity responsible for the keys (O)
    - The tax ID number of the organization responsible for the keys (OrganizationIdentifier)
    - The country where the company responsible for the keys carries out the activity. (C)

The ROOT certificates have a descriptive name that identifies the Certification Authority and the (O) field contains the name of the organization responsible for the Certification Authority.

3.1.2 NEED FOR NAMES TO BE MEANINGFUL

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

3.1.3 PSEUDONYMS

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

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

3.1.4 RULES USED TO INTERPRET SEVERAL NAME FORMATS

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

3.1.5 UNIQUENESS OF NAMES

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

3.1.5.1 ISSUANCE OF SEVERAL NATURAL PERSON CERTIFICATES FOR THE SAME CERTIFICATE HOLDER

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

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

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

3.1.6 RECOGNITION, AUTHENTICATION, AND FUNCTION OF REGISTERED TRADEMARKS AND OTHER DISTINCTIVE SYMBOLS

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

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

1) Keys created by Camerfirma

   In software: They are given to the Subject/Signatory in person or by mail via protected files, using Standard PKCS#12. The security of the process is ensured because the access code to the PKCS #12 file, which makes it possible to install it in the applications, is delivered by a different means than the one used to receive the file.

   In SmartCard/Token QSCD: The keys can be delivered by Camerfirma to the Subject/Signatory, directly or through a registry authority on a Qualified Signature Creation Device (QSCD) of the SmartCard/Token type that complies with the requirements set out in Annex II of the eIDAS Regulation.

   In a centralized platform (QSCD or Non-QSCD): Camerfirma uses a remote key storage system based on a FIPS 140-2 Level 3 HSM, which allows the Subject/Signatory (or Subject/Signatory/Creator of the Seal, in the case of a legal entity) to access the key under their exclusive control (or under their control, in the case of a legal entity). In the case of a centralized QSCD platform, it complies with the requirements set out in Annex II of the eIDAS Regulation. This type of storage is not performed for SSL/TLS secure server certificates.

2) Keys created by the Signatory

   The Signatory has a key generation mechanism, either software or hardware. These keys are generated in an external device that is not managed by Camerfirma, so Camerfirma cannot guarantee that the device is qualified (QSCD) and is therefore classified as non-qualified (Non-QSCD). The proof of possession of the private key in these cases is the request received, containing the public key, by Camerfirma in PKCS #10 format.

3.2.2 AUTHENTICATION OF ORGANIZATION IDENTITY

3.2.2.1 IDENTITY

Before the issue and delivery of a certificate issued to a legal person or 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 the Spanish language indicating the existence of the entity in that country.

The Registration Agencies employed for organization identification are:

- Spain:
  - Registro Mercantil.
  - Agencia tributaria.
- Perú:
  - Superintendencia Nacional de Aduanas y de Administración Tributaria.
  - Registro Mercantil de Panamá.

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 REGISTROS 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: Before issuance and delivery of a certificate, the verification of the personal identity of the applicant 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 o 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 not residing in Spain:
  - Passport.

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

- Peruvian nationality:
  - Documento Nacional de Identidad.
- Foreigners residing in Perú:
  - Carnet de Extranjería.

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 does not have his full mental abilities.

Control over the e-mail 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 by 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 Verification Point. 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 before 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 about the assurance levels 'substantial' or 'high' (of eIDAS Regulation). Electronic identification systems notified by the Member States under Article 9.1 of the eIDAS Regulation will be accepted. In the case of Spain, the electronic DNI will be accepted.

3) Using a certificate of a qualified electronic signature issued by a Camerfirma CA or another Provider, for which the natural person has been identified in person by the issuer Provider, either directly or by relying on a third party by national law or using electronic identification means by 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 the national level which provide equivalent assurance in terms of reliability to physical presence, by the applicable regulation, in particular the conditions and technical requirements established in Orden ETD / 465/2021, of May 6, 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 confirmed 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 holds an 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 by 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 authorized by the Certification Authority after reviewing the objective characteristics of their identity documents in terms of certainty of identification, security of the Issuing Authority 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 a pre-existing relationship, in which, for the identification of the interested party, the means indicated in point 1 were used and the period 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 Representative of a Legal Entity with general powers of representation – QCP-n-qscd in QSCD SmartCard/Token, QCP-n-qscd in QSCD Cloud, or QCP-n in Non-QSCD Qualified Certificate for a Representative of a Non-Legal Entity with general powers of representation – QCP-n-qscd in QSCD SmartCard/Token, QCP-n-qscd in QSCD Cloud, or QCP-n in Non-QSCD Qualified Certificate for a Voluntary	Evidence on the Subject/Signatory's representation powers concerning the entity, by providing documentation showing their powers of representation depending on the type of entity. This information is published in the RA's operating manuals and on Camerfirma's website.

Representative of a Legal Entity before the Public Administrations - QCP-n-qscd in QSCD SmartCard/Token, QCP-n-qscd in QSCD Cloud, or QCP-n in Non-QSCD Qualified Certificate for a Voluntary Representative of a Non-Legal Entity before the Public Administrations - QCP-n-qscd in QSCD SmartCard/Token, QCP-n-qscd in QSCD Cloud, or QCP-n in Non-QSCD Qualified Certificate for Special Representative of a Legal Entity - QCP-n-qscd in QSCD SmartCard/Token, QCP-n-qscd in QCP-n-qscd in QSCD Cloud, or QCP-n in Non-QSCD Qualified Certificate for Special Representative of a Non-Legal Entity - QCP-n-qscd in QSCD SmartCard/Token, QCP-n-qscd in QSCD Cloud, or QCP-n in Non-QSCD	
Qualified Corporate Certificate - QCP-n-qscd in QSCD SmartCard/Token, QCP-n-qscd in QSCD Cloud, and QCP-n in Non-QSCD	Usually, an authorization is signed by the entity's Legal Representative.
Qualified Corporate Certificate for Self-employed - QCP-n-qscd in QSCD SmartCard/Token, QCP-n-qscd in QSCD Cloud, or QCP-n in Non-QSCD Qualified Corporate Certificate for Chartered Self-employed – QCP-n-qscd in QSCD SmartCard/Token, QCP-n-qscd in QSCD Cloud, or QCP-n in Non-QSCD Legal Person Certificate - Registered Professional Attribute	Documentation accrediting the status of Self-Employed under the Economic Activity regime, and if you are a professional member of a professional association (subscription in force). Additionally, optionally, documentation accrediting the registered trade name under which the activity is carried out.
Digital Seal	Authorization to request the certificate by someone with sufficient power of representation for the signing entity. Certificate or query from the Companies Registry to check the incorporation and legal status of the entity and the appointment and term of office of the authorizing person.
Public employee and Seal	The identity document of the person who is

	acting on behalf of the Public Administration, public body, or entity is required. The responsible Applicant/person shall be identified by the RA with his/her ID and authorization from the responsible person, indicating that it is a public employee or appointment in the Official State Gazette where this person's Tax ID No. appears.
TSU or codesign	Authorization to request the certificate by someone with sufficient power of representation for the signing entity. Certificate or query from the Companies Registry to check the incorporation and legal status of the entity and the appointment and term of office of the authorizing person.

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 internal Management 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 IN RA OPERATOR CERTIFICATES (NATURAL PERSON)

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

3.2.5.5 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 under Spanish law.

3.2.5.6 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 outlined in the applicable agreement.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

The re-key request 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.

Under AC CAMERFIRMA PERÚ CERTIFICADOS - 2016, the "re-key requests" process is called "re-issuance" as indicated by the Peruvian standard, although under said CA, processes of re-issuance of certificates will not be executed.

3.3.1 IDENTIFICATION AND AUTHENTICATION FOR ROUTINE RE-KEY

The identification of a renewal application is made through the certificate to be renewed or based on a pre-existing relationship. In both cases, the applicant's identity or other permanent circumstances must already be registered with Camerfirma and the identification of the interested party must have been carried out in person for less than five years.

For the component certificates read: electronic seal, code signing no renewals are made.

Entity certificates of intermediate CA, TSU, TSA ... etc. they are made through a specific renewal ceremony.

3.3.2 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY AFTER REVOCATION

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

Exception: When the renewal takes place on final entity certificates due to a certificate replacement process or an issuing error or a loss, the certificate can be renewed following a revocation, as long as it shows the current situation. The supporting documentation submitted to issue the replaced

certificate is reused and a physical appearance (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 4.9.3 of this document.

Camerfirma, or any of the entities that comprise it, may, on their 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

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

4.1 CERTIFICATE APPLICATION

4.1.1 WHO CAN SUBMIT A CERTIFICATE APPLICATION

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

4.1.2 ENROLLMENT PROCESS AND RESPONSIBILITIES

4.1.2.1 WEB FORMS

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

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

The form allows for the inclusion of a CSR (PKCS #10) if the user has created the keys on an external device not managed by Camerfirma.

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

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

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

There are special procedures where the registry operator delivers the conditions of use to the registrant on paper or by e-mail.

4.1.2.2 BATCHES

The Camerfirma STATUS® platform also allows batch request circuits. In this case, the applicant

sends the RA a file with a structure designed by Camerfirma containing the applicants' details. The RA uploads these requests in the management application.

4.1.2.3 APPLICATIONS FOR FINAL-ENTITY CERTIFICATES IN HSM, TSU, AND SUBORDINATE CA

Applications for issuing certificates in HSM, TSU, or Subordinate CA are made through a sales quotation at a sales area by writing to equipo.comercial@camerfirma.com.

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

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

- Statement from the applicant indicating that the keys have been generated within a hardware device and/or a technical report from a third party (service provider) certifying this process. Camerfirma provides the statement forms for Signatories and third parties.
- Records from key creation events indicating:
    - The process followed to create the keys.
    - The people involved.
    - The environment in which it was created.
    - The HSM device used (model and make).
    - Security policies employed: (size of keys, key creation parameters, exportable/not exportable, and any other relevant information).
    - The PKCS#10 request was generated.
    - Any incidents and solutions.
- Device specifications: The technical data sheet of the devices may be acceptable.

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

4.1.2.4 APPLICATIONS VIA WEB SERVICES (WS) LAYER

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

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

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

4.1.2.5 *CROSS CERTIFICATION REQUEST*

Camerfirma can perform cross-certification at the request of a client.

Camerfirma will evaluate the request and request the corresponding audits that certify that the linked system meets technical, operational, and legal standards that are comparable.

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

4.2 PROCESSING THE CERTIFICATION REQUEST

4.2.1 PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS

End entity certificates:

- Once a certificate has been requested, the RA operator, using access to the management platform (STATUS), shall verify that the information provided is consistent.
- The operator of the platform has an internal management certificate issued for these operations and that is obtained after a training and evaluation process.
- The certificate used by the registry operator is considered multi-factor access used not only for access to the PKI management platform (STATUS) but also to approve each request for issuance of a certificate by making an electronic signature.

Subordinate CA certificates:

- Through commercial acceptance corresponding to a client's request.

4.2.2 APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS

End entity certificates:

- The registry operator views the requests pending processing and those that have been assigned.
- The RA operator waits for the Subject/Signatory to present the corresponding documentation.
- In applications via the WS layer, the request is authenticated at origin, and the certificate is issued by the platform when the origin and authentication are correct.
- If the information is not correct, the RA rejects the request. If the data is verified correctly,

the Registration Authority approves the issuance of the certificate using a digital signature with its operator certificate.

Subordinate CA certificates:

- Through commercial acceptance corresponding to a client's request.

4.2.3 TIME TO PROCESS CERTIFICATE APPLICATIONS

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

The applications submitted by the Camerfirma STATUS® platform are validated once the supporting documentation associated with the certificate profile has been verified. Camerfirma will proceed as long as it is feasible to eliminate requests older than one year.

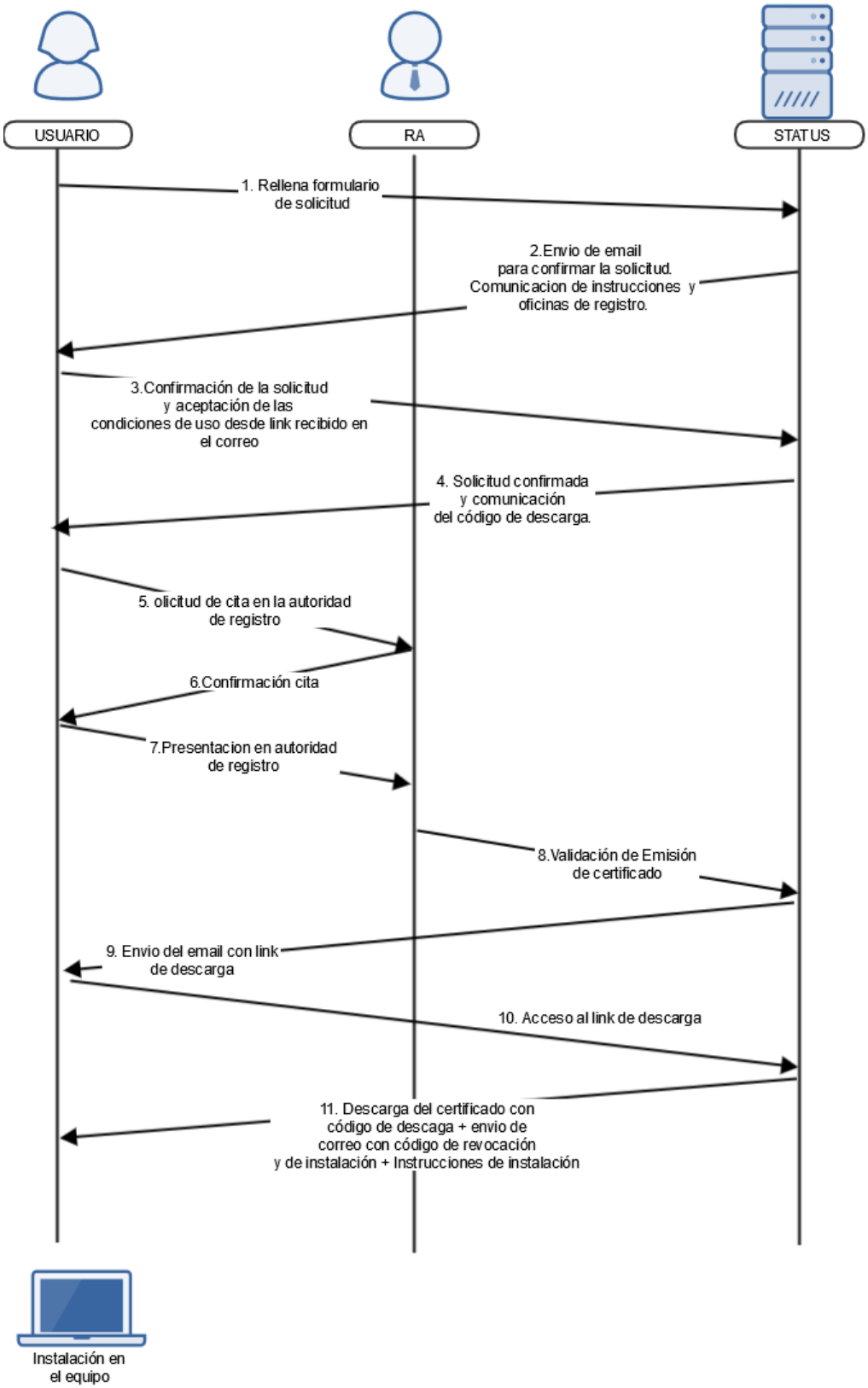
There are no stipulated deadlines for resolving a Subordinate CA certificate or cross-certification application.

4.3 CERTIFICATE ISSUANCE

4.3.1 CA ACTIONS DURING CERTIFICATE ISSUANCE

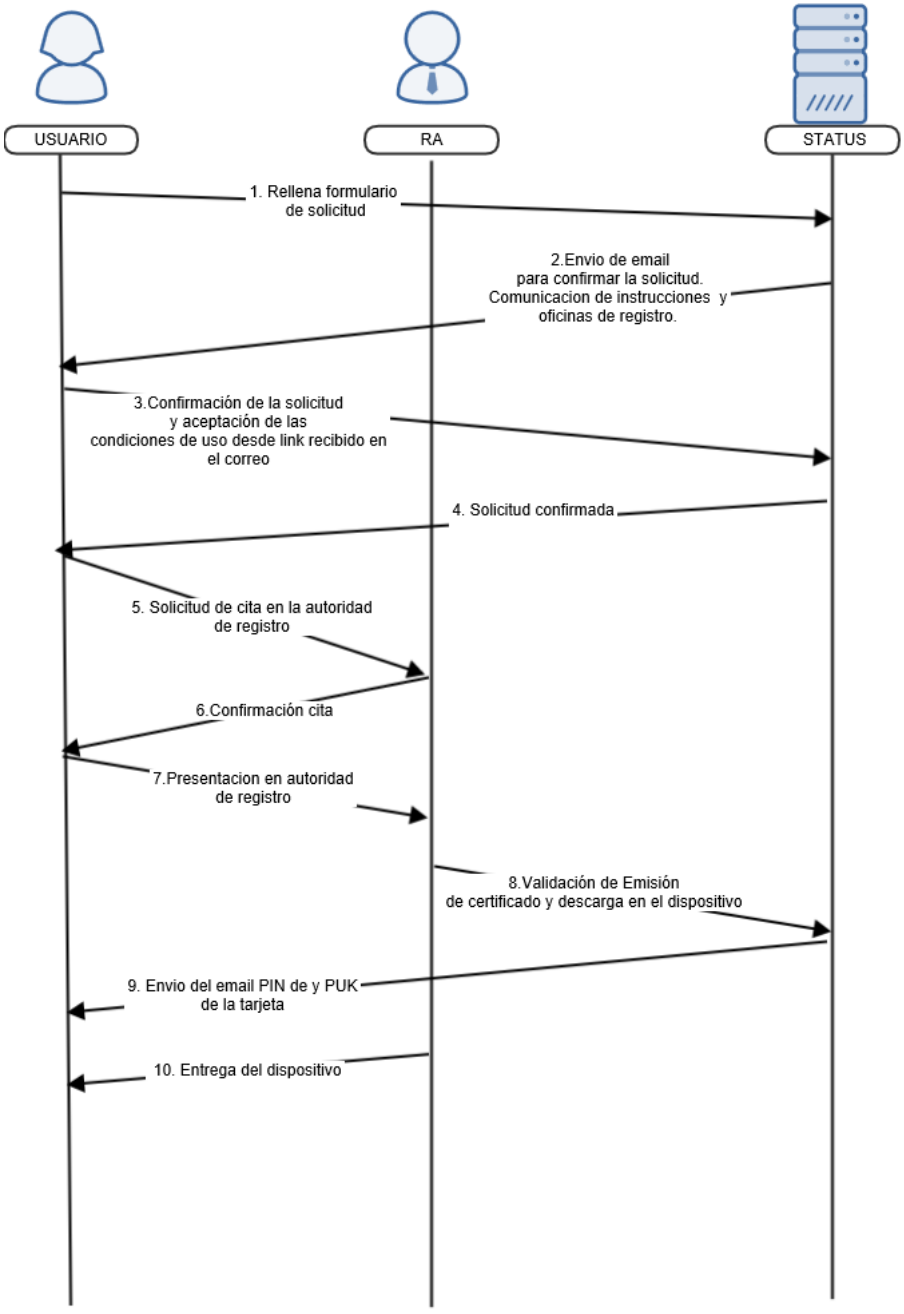
4.3.1.1 CERTIFICATES VIA SOFTWARE

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


USUARIO
RA
STATUS
1. Rellena formulario de solicitud
2.Envio de email para confirmar la solicitud. Comunicacion de instrucciones y oficinas de registro.
3.Confirmación de la solicitud y aceptación de las condiciones de uso desde link recibido en el correo
4. Solicitud confirmada y comunicación del código de descarga.
5. olicitud de cita en la autoridad de registro
6.Confirmación cita
7.Presentacion en autoridad de registro
8.Validación de Emisión de certificado
9. Envio del email con link de descarga
10. Acceso al link de descarga
11. Descarga del certificado con código de descaga + envio de correo con código de revocación y de instalación + Instrucciones de instalación
Instalación en el equipo

4.3.1.2 CERTIFICATES VIA HW (QUALIFIED SIGNATURE CREATION DEVICE OR SECURE CRYPTOGRAPHIC DEVICE)

4.3.1.2.1 CRYPTOGRAPHIC SMARTCARD OR TOKEN



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

The Registration Authority operator chooses which security card to use to create the keys. For this

purpose, the operator's workstation is configured with the CSP (Cryptographic Service Provider). Camerfirma currently allows several types of USB cards and tokens, all QSCD certified (Qualified Signature Creation Device).

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

4.3.1.3 CERTIFICATES ISSUED THROUGH WEB SERVICES REQUESTS

The requests can be received employing suitably signed calls to the service layer of the WS of the Camerfirma STATUS® platform according to section 4.1.2.4.

4.3.1.4 CERTIFICATES ISSUED ON A CENTRALIZED PLATFORM

Once the application is approved, the Signatory or the Applicant receives an email with the notification of this fact and with the Proceed to the generation and download of the certificate in the centralized device (HSM).

If the device is certified as a qualified signature creation or seal creation device the certificate shall contain the policy OID 1.3.6.1.1.4.1.17326.99.18.1 indicating that the private key associated with the certificate resides in a QCQSCDManagedOnBehalf device and complies with ETSI TS 119 431-1 for management on behalf of the signatory. If the device is not certified as a qualified signature creation or seal creation device the certificate shall not contain the OID 1.3.6.1.1.4.1.17326.99.18.1 but shall contain the policy OID 1.3.6.1.4.4.1.17326.99.21.2 to indicate that the device is not qualified.

Certificates that include the policy OID 1.3.6.1.1.4.1.17326.99.18.1 also include a Camerfirma policy OID indicating the certificate policy under which it is issued, which will be policy category 1.3.6.1.1.4.1.17326.x.x.x.x.x.1.

Certificates that include the policy OID 1.3.6.1.1.4.1.17326.99.21.2 also include a Camerfirma policy OID indicating the certificate policy under which it is issued, which will be policy category 1.3.6.1.1.4.1.17326.x.x.x.x.x.2.

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].

4.3.2 NOTIFICATION TO SUBSCRIBER BY THE CA OF ISSUANCE OF CERTIFICATE

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

Intermediate entity certificates (Subordinated CA) are issued under the execution of a key ceremony and are subsequently delivered to the representative of the organization holding the certificate.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE

Once the certificate has been delivered or downloaded, the user has a period of 14 calendar days to check that it has been correctly issued (to determine whether the data is correct and corresponds to reality); once this period has elapsed, the issued certificate is considered to be accepted.

By accepting the certificate, the accuracy of its content is confirmed and assumed, with the consequent obligations derived from this about the CA or any third party that in good faith relies on the content of the Certificate.

If the certificate has not been issued correctly for technical reasons or due to any difference between the data supplied and the content of the certificate, this must be reported immediately to the CA so that it can be revoked and a new certificate can be issued. The CA will issue a new certificate free of charge if the difference between the data is caused by an error not attributable to the user.

4.4.2 PUBLICATION OF THE CERTIFICATE BY THE CA

- Certificates issued are published at https://www.camerfirma.com/ayuda/utilidades/validacion-de-certificados/
- Camerfirma distributes its Root certificates on its website: https://www.camerfirma.com/ayuda/utilidades/descarga-de-claves-publicas/
- Camerfirma issues its Subordinate CA certificates on its website: https://www.camerfirma.com/politicas-de-certificacion-ac-camerfirma/
- Camerfirma distributes its OCSP certificates on its website: https://www.camerfirma.com/servicios-y-soluciones/respondedor-ocsp/
- Camerfirma distributes its TSA certificates on its website: https://www.camerfirma.com/servicios-y-soluciones/sellado-de-tiempo/

4.4.3 NOTIFICATION OF THE ISSUANCE TO THIRD PARTIES

No stipulation.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 SUBSCRIBER PRIVATE KEY AND CERTIFICATE USAGE

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

CA	Key Usage	Extended Key Usage	Basic Constraints
CHAMBERS OF COMMERCE ROOT **CHAMBERS OF COMMERCE ROOT - 2008** **CHAMBERS OF COMMERCE ROOT – 2016**	critical, cRLSign, keyCertSign	-	critical,CA:true
AC CAMERFIRMA CERTIFICADOS CAMERALES **AC CAMERFIRMA FOR NATURAL PERSONS - 2016**	critical, cRLSign, keyCertSign	emailProtection clientAuth	critical,CA:true, pathlen:2
Qualified Citizen Certificate - QCP-n-qscd in QSCD SmartCard/Token, QCP-n-qscd in QSCD Cloud and QCP-n in Non-QSCD	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
Qualified Corporate Certificate - QCP-n-qscd in QSCD SmartCard/Token, QCP-n-qscd in QSCD Cloud and QCP-n in Non-QSCD Qualified Corporate Certificate for Self-employed - QCP-n-qscd in QSCD SmartCard/Token, QCP-n-qscd in QSCD Cloud and QCP-n in Non-QSCD Qualified Corporate Certificate for Chartered Self-employed – QCP-n-qscd in QSCD SmartCard/Token, QCP-n-qscd in QSCD Cloud and QCP-n in Non-QSCD	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
Qualified Certificate for a Representative of a Legal Entity with general powers of representation – QCP-n-qscd in QSCD SmartCard/Token, QCP-n-	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false

qscd in QSCD Cloud and QCP-n in Non-QSCD			
Qualified Certificate for a Representative of a Non-Legal Entity with general powers of representation – QCP-n-qscd in QSCD SmartCard/Token, QCP-n-qscd in QSCD Cloud and QCP-n in Non-QSCD	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/Token, QCP-n-qscd in QSCD Cloud and QCP-n in Non-QSCD	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/Token, QCP-n-qscd in QSCD Cloud and QCP-n in Non-QSCD	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
Qualified Certificate for Special Representative of a Legal Entity - QCP-n-qscd in QSCD SmartCard/Token, QCP-n-qscd in QSCD Cloud and QCP-n in Non-QSCD	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
Qualified Certificate for Special Representative of a Non-Legal Entity - QCP-n-qscd in QSCD SmartCard/Token, QCP-n-qscd in QSCD Cloud and QCP-n in Non-QSCD	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
Qualified Certificate of Signature for Public Employee. High Level.	critical, contentCommitment	-	critical,CA:false
Qualified Certificate of Authentication for Public Employee. High Level.	critical, digitalSignature	emailProtection clientAuth	critical,CA:false

Qualified Certificate of Encipherment for Public Employee. High Level.	critical, keyEncipherment, dataEncipherment	emailProtection clientAuth	critical,CA:false
Qualified Certificate for Public Employee. Medium Level.	critical, digitalSignature, contentCommitment , keyEncipherment	emailProtection clientAuth	critical,CA:false
Qualified Certificate of Signature for Public Employee under a pseudonym. High Level.	critical, contentCommitment	-	critical,CA:false
Qualified Certificate of Authentication for Public Employee under a pseudonym. High Level.	critical, digitalSignature	emailProtection clientAuth	critical,CA:false
Qualified Certificate of Encipherment for Public Employee under a pseudonym. High Level.	critical, digitalSignature, contentCommitment , keyEncipherment	emailProtection clientAuth	critical,CA:false
AC CAMERFIRMA FOR LEGAL PERSONS – 2016	critical, cRLSign, keyCertSign	emailProtection clientAuth	critical,CA:true, pathlen:2
Qualified Digital Seal Certificate	critical, digitalSignature, contentCommitment , keyEncipherment	emailProtection clientAuth	critical,CA:false
Digital Seal Certificate	critical, digitalSignature, contentCommitment , keyEncipherment	emailProtection clientAuth	critical,CA:false
Qualified Digital Seal Certificate for Public Administrations. High Level.	critical, digitalSignature, contentCommitment , keyEncipherment	emailProtection clientAuth	critical,CA:false
Qualified Digital Seal Certificate for Public Administrations. Medium Level.	critical, digitalSignature, contentCommitment , keyEncipherment	emailProtection clientAuth	critical,CA:false
AC CAMERFIRMA TSA - 2016	critical, cRLSign, keyCertSign	timeStamping	critical,CA:true, pathlen:2
Qualified TSU Certificate	critical,	timeStamping	critical,CA:false

	contentCommitment		
AC CAMERFIRMA AAPP II – 2014	critical, cRLSign, keyCertSign	emailProtection clientAuth serverAuth	critical,CA:true, pathlen:2
Recognized certificate of the electronic seal of Administration, body or entity of public law, high level	critical, digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment	clientAuth emailProtection	critical,CA:false
Recognized certificate of the electronic seal of Administration, body or entity of public law, medium level	critical, digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment	clientAuth emailProtection	critical,CA:false
Recognized public employee certificate, high level, signature	critical, nonRepudiation	-	critical,CA:false
Recognized public employee certificate, high-level, authentication	critical, digitalSignature	clientAuth emailProtection	critical,CA:false
Recognized public employee certificate, high-level, encryption	critical, keyEncipherment, dataEncipherment	clientAuth emailProtection	critical,CA:false
Recognized public employee certificate, medium level	critical, digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment	clientAuth emailProtection	critical,CA:false
AC CAMERFIRMA CORPORATE SERVER II – 2015	critical, cRLSign, keyCertSign	emailProtection clientAuth serverAuth	critical,CA:true, pathlen:2
Enterprise Electronic Seal Certificate Software - keys generated by the TSP	critical, digitalSignature, keyEncipherment, dataEncipherment, keyAgreement, nonRepudiation	clientAuth emailProtection	critical,CA:false
Enterprise Electronic Seal Certificate Software - keys	critical, digitalSignature,	clientAuth emailProtection	critical,CA:false

generated by the user	keyEncipherment, dataEncipherment, keyAgreement, nonRepudiation		
Camerfirma Codesign II – 2014	critical, cRLSign, keyCertSign	codeSigning msCodeCom	critical,CA:true, pathlen:2
Certificado de firma de código	critical, digitalSignature, nonRepudiation	codeSigning msCodeCom	critical,CA:false
Camerfirma TSA – 2013	critical, cRLSign, keyCertSign	-	critical,CA:true, pathlen:2
Camerfirma TSA II – 2014	critical, cRLSign, keyCertSign	timeStamping	critical,CA:true, pathlen:2
AC Camerfirma Express Corporate Server	critical, cRLSign, keyCertSign	-	critical,CA:true, pathlen:11
GLOBAL CHAMBERSIGN ROOT - 2016	critical, cRLSign, keyCertSign	-	critical,CA:true
AC CAMERFIRMA COLOMBIA - 2016	critical, cRLSign, keyCertSign	-	critical,CA:true, pathlen:2
CAMERFIRMA COLOMBIA SAS CERTIFICADOS - 001	critical, cRLSign, keyCertSign	emailProtection clientAuth	critical,CA:true, pathlen:1
CAMERFIRMA COLOMBIA SAS CERTIFICADOS - 002	critical, cRLSign, keyCertSign	emailProtection clientAuth	CA:TRUE, pathlen:0
AC CAMERFIRMA PERÚ - 2016	critical, cRLSign, keyCertSign	-	critical,CA:true, pathlen:2
AC CAMERFIRMA PERÚ CERTIFICADOS – 2016	critical, cRLSign, keyCertSign	emailProtection clientAuth	critical,CA:true, pathlen:1
Legal Entity Certificate - Entity Membership Attribute	critical, digitalSignature, contentCommitment , keyEncipherment	emailProtection clientAuth	critical,CA:false
Legal Entity Certificate - Representative Attribute	critical, digitalSignature, contentCommitment , keyEncipherment	emailProtection clientAuth	critical,CA:false
Legal Entity Certificate	critical, digitalSignature,	emailProtection	critical,CA:false

	contentCommitment, keyEncipherment	clientAuth	
Legal Entity Certificate - Electronic Invoice Attribute	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
Natural Person Certificate	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
Companies Electronic Seal Certificate for an automatized agent	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
Legal Person Certificate - Registered Professional Attribute	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
AC CAMERFIRMA – 2009	critical, cRLSign, keyCertSign	-	critical,CA:true, pathlen:2
Entitat de Certificació de l'Administració Pública Andorrana-19	critical, cRLSign, keyCertSign	emailProtection clientAuth	critical,CA:true, pathlen:0
MULTICERT SSL Certification Authority 001	critical, cRLSign, keyCertSign	clientAuth serverAuth	critical,CA:true, pathlen:0
GLOBAL CORPORATE SERVER	critical, cRLSign, keyCertSign	-	critical,CA:true
InfoCert Organization Validation CA 3	critical, cRLSign, keyCertSign	clientAuth serverAuth	critical,CA:true, pathlen:0
InfoCert Organization Validation 2019 CA 3	critical, cRLSign, keyCertSign	clientAuth serverAuth	critical,CA:true, pathlen:0
AC Camerfirma Portugal – 2015	critical, cRLSign, keyCertSign	-	critical,CA:true, pathlen:3

DigitalSign Primary CA	critical, cRLSign, keyCertSign	-	critical,CA:true, pathlen:1
DigitalSign CA	critical, cRLSign, keyCertSign	emailProtection clientAuth	critical,CA:true, pathlen:0
DigitalSign TSA CA	critical, cRLSign, keyCertSign	timeStamping	critical,CA:true, pathlen:0
AC Camerfirma	critical, cRLSign, keyCertSign	-	critical,CA:true, pathlen:11
RACER	critical, cRLSign, keyCertSign	-	critical,CA:true, pathlen:10
AC Camerfirma de Ciudadano	critical, digitalSignature, keyEncipherment, dataEncipherment, keyAgreement, nonRepudiation	clientAuth emailProtection	critical,CA:false
AC Camerfirma de Ciudadano - Hardware - claves generadas por el PSC	critical, digitalSignature, keyEncipherment, dataEncipherment, keyAgreement, nonRepudiation	clientAuth emailProtection	critical,CA:false
AC Camerfirma de Ciudadano - Hardware - claves generadas por el usuario	critical, digitalSignature, keyEncipherment, dataEncipherment, keyAgreement, nonRepudiation	clientAuth emailProtection	critical,CA:false

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

For remote signature or remote seal certificates, the Subject/Signer or Seal Subject/Creator must securely retain the remote signature authentication tools and/or devices. You must also keep the private key activation PIN of the remote signature certificate under your exclusive control and separately from authentication passwords or authentication devices. Finally, you must ensure that you maintain the privacy and preservation of the certificate revocation PIN. The Subject/Signer and Seal Subject/Creator should not create signatures with suspended or revoked certificate private keys or use revoked CA certificates.

4.5.2 RELYING PARTY PUBLIC KEY AND CERTIFICATE USAGE

The relying parties must access and use the public key and the certificate as stipulated in this CPS and as indicated in the "Terms of Use" either in a physical document or by acceptance in the issuance process.

4.6 CERTIFICATE RENEWAL

4.6.1 CIRCUMSTANCE FOR CERTIFICATE RENEWAL

A certificate must be renewed before the expiration date of the certificate to be renewed. Once renewed Camerfirma issues the renewed certificate with a start date equal to the expiration date of the certificate to be renewed.

(Applies only to Camerfirma Perú) By Peruvian regulations, certificate re-issuance can only be carried out under the following circumstances:

- For Natural Person Certificates: the re-issuance can only be carried out once, for certificates whose expiration date is less than or equal to one year, before the expiration of the validity period. The reissued certificate must have a maximum validity period of one year.
- For Legal Person Certificates - Attributes: the reissue can only be carried out once, for certificates whose expiration date is less than or equal to two years. The reissued certificate must have a maximum validity period of one year.
- For Company Electronic Seal Certificates for automated Agents: the re-issuance can only be carried out once when a digital certificate has been revoked before the expiration of its validity period.

However, these CPS rules that Camerfirma does not offer renewal services for code signing certificates, electronic seal certificates or certificates issued under the AC CAMERFIRMA PERÚ CERTIFICADOS - 2016. Renewals are called “reissues” by the Peruvian standard.

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

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

TSU certificates are issued for five years with private key usage of four years and ten months. These TSU certificates are renewed no later than two months before their expiration date.

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

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

The component end-entity certificates (corporate seal and CodeSign) do not currently support renewal. In this case, a new issuance must be done.

4.6.2 WHO MAY REQUEST RENEWAL

In those certificates where renewal is allowed, the renewal can be requested by the holder or a representative of the organization described in the certificate or the authorized person before the Registration Authority.

4.6.3 PROCESSING CERTIFICATE RENEWAL REQUESTS

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

In the case of renewal of the qualified certificates of the final entity of an individual, the issuance of a certificate without a physical presence is allowed for up to 5 years from the last face-to-face registration. Once the deadline has been set, the Signatory must carry out a face-to-face broadcast process equal to the first issue. Under these practices, if at the time of the renewal of the certificate has not elapsed more than 5 years, the physical presence of the owner will not be required.

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

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

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

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

- Once the certificate being renewed has been identified, the application gives the Signatory the old certificate details and requests confirmation. The application allows the Signatory to change the email address assigned to the certificate. If other information included in the certificate has changed, the certificate must be revoked and a new one issued.
- The request is included in the RA application. Once the operator has checked the data, the CA is requested to issue the certificate.
- As a general rule, Camerfirma issues a new certificate, taking the expiry date of the certificate being renewed as this new certificate's start date. In some cases, certificate renewal with the date at the same time of renewal, subsequently revoking the certificate to be renewed, is allowed in the emission processes through web services.

Component end-entity corporate seal certificates cannot be renewed; the process for issuing a new certificate must be followed.

4.6.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

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

4.6.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RENEWAL CERTIFICATE

As stipulated in section 4.4.1 of this document.

4.6.6 PUBLICATION OF THE RENEWAL CERTIFICATE BY THE CA

As stipulated in section 4.4.2 of this document.

4.6.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

In some cases, final entity certificates are sent to the national supervisors that regulate the activities of the certification authorities.

Qualified TSU certificates are notified to the national supervisor.

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

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

4.7 CERTIFICATE RE-KEY

This is the usual procedure for renewing Camerfirma certificates, by which all the processes described in this section refer to this renewal method.

Camerfirma does not allow certificate renewal without key renewal.

4.7.1 CIRCUMSTANCE FOR CERTIFICATE RE-KEY

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

4.7.2 WHO MAY REQUEST CERTIFICATION OF A NEW PUBLIC KEY

As stipulated in section 4.6.2 of this document.

4.7.3 PROCESSING CERTIFICATE RE-KEYING REQUESTS

As stipulated in section 4.6.3 of this document.

4.7.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

As stipulated in section 4.6.4 of this document.

4.7.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RE-KEYED CERTIFICATE

As stipulated in section 4.6.5 of this document.

4.7.6 PUBLICATION OF THE RE-KEYED CERTIFICATE BY THE CA

As stipulated in section 4.6.6 of this document.

4.7.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

As stipulated in section 4.6.7 of this document.

4.8 CERTIFICATE MODIFICATION

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

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

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

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

4.8.1 CIRCUMSTANCE FOR CERTIFICATE MODIFICATION

Not applicable.

4.8.2 WHO MAY REQUEST CERTIFICATE MODIFICATION

Not applicable.

4.8.3 PROCESSING CERTIFICATE MODIFICATION REQUESTS

Not applicable.

4.8.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

Not applicable.

4.8.5 CONDUCT CONSTITUTING ACCEPTANCE OF MODIFIED CERTIFICATE

Not applicable.

4.8.6 PUBLICATION OF THE MODIFIED CERTIFICATE BY THE CA

Not applicable.

4.8.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

Not applicable.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

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

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

The maximum period of suspension of a certificate is 7 calendar days. In case of reaching the maximum period of suspension and the certificate has not been activated, the system automatically revokes the certificate definitively with an "unspecified" cause.

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

Camerfirma maintains the certificates on the revocation list until the end of their validity. When this

occurs, they are removed from the list of revoked certificates. Camerfirma will only eliminate a certificate from the revocation list in either of the following situations:

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

In case of revocation of an intermediate CA, expired certificates cannot be consulted by the CRL since they leave it, but they can be consulted either by OCSP or by consulting the revocation information on the Camerfirma website. Non-expired certificates can be consulted either by CRL, OCSP or on the Camerfirma website. Information on the status of certificates will be maintained for at least 15 years from its expiration date.

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

Revoked certificates cannot be used under these practices.

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

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

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

4.9.1 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.

Due to circumstances affecting key or certificate security:

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

person/entity responsible for the certificate.

- There is a misuse of the certificate by the Signatory or person/entity responsible for the certificate or failure to keep the private key secure.

Due to circumstances affecting the security of the cryptographic device:

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

Some circumstances that affect the Signatory or person/entity responsible for the certificate:

- The relationship is terminated between the Certification Authority and the Signatory or person/entity responsible for the certificate.
- There are changes to or termination of the underlying legal relationship or cause for issuing the certificate to the Signatory or person/entity responsible for the certificate.
- The applicant breaches part of the requirements established for requesting the certificate.
- The Signatory or person responsible for the certificate breach part of their obligations, responsibility and guarantees established in the legal document or this CPS.
- The sudden incapacity or death of the Signatory or person/entity responsible for the certificate.
- There is a termination of the legal entity that is the Signatory of the certificate and expiry of the authorisation provided by the Signatory to the person/entity responsible for the certificate, or termination of the relationship between the Signatory and the person/entity responsible for the certificate.
- The Signatory requests revocation of the certificate by the provisions of this CPS.
- Firm resolution of the competent administrative or judicial Authority.
- The signer indicates that the original certificate request was not authorized and does not grant the authorization retroactively.

Other circumstances:

- Suspension of the digital certificate for a longer period than established in this CPS.
- For the issuance of a certificate that does not meet the requirements outlined in this CPS.
- Termination of the Certification Authority's service, by the corresponding section of this CPS.
- The certificate was issued in violation of the valid version of the requirements set by the *Mozilla Root Store Policy*.

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

- If the certificate holder or the natural person applying for the certificate for a legal entity, a signed statement must be provided indicating the certificate to be revoked and the reason for this request and identification must be provided to the RA.
- If the revocation is requested by a third party, it must present authorisation from the natural person certificate holder or the legal representative of the legal entity certificate holder. The third party must indicate the reasons for requesting revocation of the certificate and identify itself to the RA.
- If the Entity requesting revocation is associated with the certificate holder due to termination of the relationship with it, this circumstance must be proven (revocation of powers, contract termination, etc.) and they applicant must identify him/herself to the RA as authorised to represent the Entity.

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

4.9.2 WHO CAN REQUEST REVOCATION

Certificate revocation can be requested by:

- The Subject/Signatory.
- The responsible Applicant.
- The Entity (via a representative), or through an electronic seal backed by a certificate issued by Camerfirma in the name of the Entity.
- The RA or the 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.

4.9.3 PROCEDURE FOR REVOCATION REQUEST

Requests for revocation by the Subject/Signatory, the Responsible Applicant or the Entity must be made:

- Via the online Revocation Service, by accessing the revocation service on Camerfirma's website and entering the Revocation PIN number. https://www.camerfirma.com/ayuda/utilidades/revocacion-de-certificados/

  If the revocation request cannot be made through the online revocation service –due to unavailability or failure of the service, or because the Revocation PIN is not available and cannot be recovered in the email from which the certificate issuance was requested–, the revocation request may be made by communicating with the RA or CA by email and additionally by telephone. In this case, the operator handling the revocation request shall

identify the applicant by means of the procedures it deems appropriate.

- Through a request sent to a Camerfirma Web Service, digitally signed with an electronic seal certificate of legal entity type issued by Camerfirma to the Entity's name, or with an electronic signature certificate issued by Camerfirma to the Entity's representative's name. This modality may be used by the Entities that require it to revoke certificates issued to natural persons linked to the Entity. In these cases, the digitally signed request will be saved as evidence of the revocation request.
- By physically going to the RA during business hours showing the ID of the Subject/Signatory, responsible Applicant or representative of the Entity.
- By sending Camerfirma a document signed by a representative with sufficient representation powers for the entity requesting certificate revocation. This form must be used to revoke Subordinate CA and TSU certificates.

Camerfirma stores all the information relating to certificate revocation processes on its website. https://www.camerfirma.com/ayuda/utilidades/revocacion-de-certificados/

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

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

4.9.4 REVOCATION 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, by 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 these 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

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

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

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

4.9.7 CRL ISSUANCE FREQUENCY

CA	Issuance frequency (days)	Duration (days)
CHAMBERS OF COMMERCE ROOT **CHAMBERS OF COMMERCE ROOT – 2008** **CHAMBERS OF COMMERCE ROOT – 2016**	Maximum 365	365
AC CAMERFIRMA FOR NATURAL PERSONS – 2016 AC CAMERFIRMA FOR LEGAL PERSONS – 2016 AC CAMERFIRMA TSA – 2016 IVSIGN CA AC CAMERFIRMA AAPP II – 2014 AC CAMERFIRMA CORPORATE SERVER II – 2015 Camerfirma Codesign II – 2014 Camerfirma TSA – 2013 Camerfirma TSA II – 2014 AC Camerfirma Express Corporate Server AC CAMERFIRMA CERTIFICADOS CAMERALES	Immediate - Maximum 1	2
GLOBAL CHAMBERSIGN ROOT – 2016 **GLOBAL CHAMBERSIGN ROOT – 2008** **Global Chambersign Root**	Maximum 365	365

AC CAMERFIRMA PERÚ – 2016 AC CAMERFIRMA COLOMBIA – 2016 GLOBAL CHAMBERSIGN ROOT – 2008 AC CAMERFIRMA – 2009 GLOBAL CORPORATE SERVER AC Camerfirma Portugal – 2015 DigitalSign Primary CA AC Camerfirma		
CAMERFIRMA COLOMBIA SAS CERTIFICADOS – 001 CAMERFIRMA COLOMBIA SAS CERTIFICADOS – 002 AC CAMERFIRMA PERÚ CERTIFICADOS – 2016 Entitat de Certificació de l'Administració Pública Andorrana-19 MULTICERT SSL Certification Authority 001 InfoCert Organization Validation CA 3 InfoCert Organization Validation 2019 CA 3 DigitalSign CA DigitalSign TSA CA RACER	Immediate - Maximum 1	2

4.9.8 MAXIMUM LATENCY FOR CRLS

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

4.9.9 ON-LINE REVOCATION/STATUS CHECKING AVAILABILITY

CA provides an online service to check revocations at: https://www.camerfirma.com/ayuda/utilidades/validacion-de-certificados/

Also via OCSP queries at: https://www.camerfirma.com/servicios-y-soluciones/respondedor-ocsp/

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

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

Certificates may contain more than one CRL distribution point to guarantee its availability.

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

OCSP responses are signed by an OCSP Responder certificate signed by the Issuing CA of the certificate whose revocation status is being checked.

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

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

Maximum latency to publish an OCSP revocation is 1 hour.

4.9.10 ON-LINE REVOCATION CHECKING REQUIREMENTS

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

OCSP responses are signed by the CA that issued the certificate on request; the certificate is required to validate the response. Updated certificates can be found at the link https://www.camerfirma.com/servicios-y-soluciones/respondedor-ocsp/.

4.9.11 OTHER METHODS OF DISCLOSING REVOCATION INFORMATION

Mechanisms that Camerfirma makes available to system users is published on its website https://www.camerfirma.com/ayuda/utilidades/validacion-de-certificados/.

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

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

If the certificate is suspended, a notice is sent to the Subject/Signatory by email specifying the time

of suspension and the reason. If Camerfirma does not have all the information necessary to verify its final status within this period, Camerfirma will revoke the certificate with certificate's revocation reason as "unspecified".

In the event of a certificate suspension, an email is sent to the Subject/Signatory informing the time of suspension and the cause of the suspension.

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

The suspension process does not apply to:

- TSU/TSA certificates
- CA certificates.
- RA Operator certificates.
- OCSP certificates.
- Electronic Seal certificates.

4.9.14 WHO CAN REQUEST SUSPENSION

See section 4.9.2.

4.9.15 PROCEDURE FOR SUSPENSION REQUEST

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

4.9.16 LIMITS ON SUSPENSION PERIOD

A certificate shall not be suspended for more than 7 days.

Camerfirma supervises, via Camerfirma STATUS® alert system, that the suspension period established by the CP and this CPS is not exceeded.

4.10 CERTIFICATE STATUS SERVICES

4.10.1 OPERATIONAL CHARACTERISTICS

Camerfirma provides a service for consulting issued certificates and revocation lists. These services are available to the public on its website:

https://www.camerfirma.com/ayuda/utilidades/validacion-de-certificados/.

4.10.2 SERVICE AVAILABILITY

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

4.10.3 OPTIONAL FEATURES

No stipulation.

4.11 END OF SUBSCRIPTION

The subscription to the service will end after the validity period of the certificate.

As an exception, the subscriber can maintain the current service by requesting the renewal of the certificate, within the advance period determined by this this CPS.

4.12 KEY ESCROW AND RECOVERY

4.12.1 KEY ESCROW AND RECOVERY POLICY AND PRACTICES

For certificates in SmartCard/Token it is the user who generates and keeps the private key in the cryptographic SmartCard/Token delivered by the provider.

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

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

Camerfirma does not store the private key of those certificates whose keys have been generated in a non-qualified external device not managed by Camerfirma.

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

4.12.2 SESSION KEY ENCAPSULATION AND RECOVERY POLICY AND PRACTICES

No stipulation.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 PHYSICAL SECURITY CONTROLS

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

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

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

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

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

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

5.1.1 SITE LOCATION AND CONSTRUCTION

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

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

Camerfirma uses AWS cloud for the OCSP services for the full hierarchy.

For this service, that need business continuity with RTO/RPO values close to zero, some components of the CAs services relating to the OCSP are hosted on AWS cloud in Frankfurt Europe Region.

AWS has certifications of conformity per the ISO/IEC 27001:2013, 27017:2015, 27018:2019, and ISO/IEC 9001:2015 standards.

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

5.1.2 PHYSICAL ACCESS

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

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

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

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

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

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

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

Physical access to AWS Data Centers is governed by AWS security procedures.

5.1.3 POWER AND AIR CONDITIONING

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

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

5.1.4 WATER EXPOSURE

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

5.1.5 FIRE PREVENTION AND PROTECTION

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

Cryptographic devices and supports that store Certification Entity keys have a specific and additional

fire protection system relative to the rest of the facility.

5.1.6 MEDIA STORAGE

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

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

5.1.7 WASTE DISPOSAL

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

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

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

Reference document: IN-2005-01-03-Seguridad medioambiental.

5.1.8 OFF-SITE BACKUP

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

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

Reference document: IN-2005-04-06-Procedimiento de Backups de ficheros críticos.

5.2 PROCEDURAL CONTROLS

5.2.1 TRUSTED ROLES

Roles of trust 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.

Internal Auditor:

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

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

Systems Administrator:

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

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

CA Administrator:

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

CA administrator tasks are incompatible with system tasks.

CA Operator:

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

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

RA Operator:

Responsible for approving certification requests from the Signatory.

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

RA Operator can't issue certificate to his/herself (PKI system doesn't allow it).

Revocation Officers:

Authorized to perform certificates revocation.

Revocation officers tasks are incompatible with audit tasks.

Security Manager:

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

Reference document: IN-2005-02-07 Funciones y responsabilidad del personal.

5.2.2 NUMBER OF PERSONS REQUIRED PER TASK

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

5.2.3 IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE

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

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

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

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

5.2.4 SWITCHING THE PKI MANAGEMENT SYSTEM ON AND OFF

The PKI system is formed by the following modules:

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

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

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

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

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

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

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

The module switch-off sequence is:

- Application Module.

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

The switching on process is carried out in reverse.

Reference document: IN-2005-05-01-Procedimiento para el apagado manual de equipos.

5.3 PERSONNEL CONTROLS

5.3.1 QUALIFICATIONS, EXPERIENCE, AND CLEARANCE REQUIREMENTS

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

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

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

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

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

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

Camerfirma shall not assign a trusted or managed site to a person who is not suitable for the position, especially for having been convicted of a crime or 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.

Reference documents:

- IN-2005-02-07 Funciones y responsabilidad del personal.
- IN-2005-02-17-Gestión Recursos humanos.

- IN-2008-00-09-Registros de Formación
- IN-2006-02-03-Organización para la Seguridad.

5.3.2 BACKGROUND CHECK PROCEDURES

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

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

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

5.3.3 TRAINING REQUIREMENTS

Personnel undertaking duties of trust must have been trained by Certification Policies. There is a training plan that is part of the UNE-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.

5.3.4 RETRAINING FREQUENCY AND REQUIREMENTS

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

5.3.5 JOB ROTATION FREQUENCY AND SEQUENCE

No stipulation.

5.3.6 SANCTIONS FOR UNAUTHORIZED ACTIONS

Camerfirma has established an internal penalty system, which is described in its HR policy, to be

applied when an employee undertakes unauthorized actions, which includes the possibility of dismissal.

Reference document: IN-2005-02-17-Gestión Recursos humanos.

5.3.7 INDEPENDENT CONTRACTOR REQUIREMENTS

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

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

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

Reference documents:

- IN-2006-05-02-Clausulas exigible a desarrolladores externos,
- IN-2005-02-17-Gestión Recursos humanos.

5.3.8 DOCUMENTATION SUPPLIED TO PERSONNEL

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

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

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

Reference document: IN-2005-02-17-Gestión Recursos humanos.

5.4 AUDIT LOGGING PROCEDURES

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

5.4.1 TYPES OF EVENTS RECORDED

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

The following events are recorded:

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

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

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

Camerfirma maintains a system that guarantees:

- Sufficient space for storing audit logs.

- Audit log files are not rewritten.
- That the saved information includes at least the following: event type, date and time, user executing the event and result of the process.
- The audit log files are saved in structured files that can be included in a database for subsequent data mining.

5.4.2 FREQUENCY OF PROCESSING LOG

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

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

5.4.3 RETENTION PERIOD FOR AUDIT LOGS

The Audit Log is retained by the CA for 15 years.

5.4.4 PROTECTION OF AUDIT LOG

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

They are stored in fireproof devices.

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

Audit log files can only be accessed by authorised persons.

Devices are always handled by authorised personnel.

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

5.4.5 AUDIT LOG BACKUP PROCEDURES

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

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

A copy is also kept at an external custody center.

Reference document: IN-2005-04-10-procedimiento de gestión de registros de auditoría.

5.4.6 AUDIT COLLECTION SYSTEM (INTERNAL VS. EXTERNAL)

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

5.4.7 NOTIFICATION TO EVENT-CAUSING SUBJECT

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

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

5.4.8 VULNERABILITY ASSESSMENTS

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

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

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

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

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

5.5 RECORDS ARCHIVAL

5.5.1 TYPES OF RECORDS ARCHIVED

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

- Any system audit data. PKI, TSA, OCSP and centralized key platform, qualified or unqualified, incorporating the signature events performed.

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

Camerfirma is responsible for correctly filing all this material.

5.5.2 RETENTION PERIOD FOR ARCHIVE

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

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

5.5.3 RETENTION PERIOD FOR ARCHIVE

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

Reference document: IN-2005-04-01- Procedimiento de gestión de logs.

5.5.4 ARCHIVE BACKUP PROCEDURES

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

Reference document: IN-2005-04-01- Procedimiento de gestión de logs.

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

5.5.5 REQUIREMENTS FOR TIME-STAMPING OF RECORDS

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

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

Reference document: IN-2006-04-01-Sincronización de tiempos.

5.5.6 ARCHIVE COLLECTION SYSTEM (INTERNAL OR EXTERNAL)

Reference document: IN-2005-04-10-procedimiento de gestión de registros de auditoría.

5.5.7 PROCEDURES TO OBTAIN AND VERIFY ARCHIVE INFORMATION

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

Reference document: IN-2005-04-06-Procedimiento de Backups de ficheros críticos.

5.6 KEY CHANGEOVER

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

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

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

Reference document: IN-2005-04-04-Procedimiento de cambio de claves.

5.7 COMPROMISE AND DISASTER RECOVERY

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

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

5.7.1 INCIDENT AND COMPROMISE HANDLING PROCEDURES

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

The continuity and contingency plan are drafted in document: CONF-2003-00-01 Continuidad y Disponibilidad.

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

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

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

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

5.7.3 ENTITY PRIVATE KEY COMPROMISE PROCEDURES

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 for Qualified Trusted Services.

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.

- 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

The modules used by Camerfirma to store root keys and are certified by FIPS 140-2, level 3.

Root keys are generated and managed on an offline computer in a cryptographic room.

Reference document CONF-00-2012-02-Script of CA ROOT generation xxxx where "xxxx" is the year corresponding to the creation of the key.

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

CA	Key Length	Signature Algorithm	Creation year	Expiry dd/mm/yyyy
CHAMBERS OF COMMERCE ROOT – 2016	4.096 bits	sha256WithRSAEncryption	2.016	08/04/2040
AC CAMERFIRMA FOR NATURAL PERSONS - 2016	4.096 bits	sha256WithRSAEncryption	2.016	09/03/2040
AC CAMERFIRMA FOR LEGAL PERSONS - 2016	4.096 bits	sha256WithRSAEncryption	2.016	09/03/2040
AC CAMERFIRMA TSA – 2016	4.096 bits	sha256WithRSAEncryption	2.016	09/03/2040
IVSIGN CA	4.096 bits	sha256WithRSAEncryption	2.017	16/03/2040
Chambers of Commerce Root – 2008	4.096 bits	sha1WithRSAEncryption	2.008	31/07/2038
Camerfirma AAPP II – 2014	4.096 bits	sha256WithRSAEncryption	2.014	15/12/2037
Camerfirma Corporate Server II - 2015	4.096 bits	sha256WithRSAEncryption	2.015	15/12/2037
Camerfirma Codesign II – 2014	4.096 bits	sha256WithRSAEncryption	2.014	15/12/2037
Camerfirma TSA – 2013	4.096	sha1WithRSAEncryption	2.013	19/02/2037

	bits				
Camerfirma TSA II – 2014	4.096 bits	sha256WithRSAEncryption	2.014	15/12/2037	
Chambers of Commerce Root	2.048 bits	sha1WithRSAEncryption	2.003	30/09/2037	
AC Camerfirma Certificados Camerales	2.048 bits	sha1WithRSAEncryption	2.004	09/02/2034	
AC Camerfirma Express Corporate Server	2.048 bits	sha1WithRSAEncryption	2.007	08/11/2032	
GLOBAL CHAMBERSIGN ROOT – 2016	4.096 bits	sha256WithRSAEncryption	2.016	08/04/2040	
AC CAMERFIRMA COLOMBIA – 2016	4.096 bits	sha256WithRSAEncryption	2.016	09/03/2040	
CAMERFIRMA COLOMBIA SAS CERTIFICADOS – 001	4.096 bits	sha256WithRSAEncryption	2.019	04/11/2031	
CAMERFIRMA COLOMBIA SAS CERTIFICADOS – 002	4.096 bits	sha256WithRSAEncryption	2.019	04/11/2031	
AC CAMERFIRMA PERÚ – 2016	4.096 bits	sha256WithRSAEncryption	2.016	10/03/2040	
AC CAMERFIRMA PERÚ CERTIFICADOS – 2016	4.096 bits	sha256WithRSAEncryption	2.016	09/02/2040	
Global Chambersign Root - 2008	4.096 bits	sha1WithRSAEncryption	2.008	31/07/2038	
AC Camerfirma - 2009	4.096 bits	sha1WithRSAEncryption	2.009	11/03/2029	

Entitat de Certificació de l'Administració Pública Andorrana-19	4.096 bits	sha256WithRSAEncryption	2.019	30/05/2038
MULTICERT SSL Certification Authority 001	4.096 bits	sha256WithRSAEncryption	2.018	20/05/2025
GLOBAL CORPORATE SERVER	4.096 bits	sha256WithRSAEncryption	2.017	20/05/2037
InfoCert Organization Validation CA 3	4.096 bits	sha256WithRSAEncryption	2.017	02/07/2035
InfoCert Organization Validation 2019 CA 3	4.096 bits	sha256WithRSAEncryption	2.019	14/11/2031
AC Camerfirma Portugal – 2015	4.096 bits	sha256WithRSAEncryption	2.015	21/11/2037
DigitalSign Primary CA	4.096 bits	sha512WithRSAEncryption	2.015	09/11/2037
DigitalSign CA	4.096 bits	sha512WithRSAEncryption	2.015	30/10/2037
DigitalSign TSA CA	4.096 bits	sha512WithRSAEncryption	2.015	30/10/2037
Global Chambersign Root	2.048 bits	sha1WithRSAEncryption	2.003	30/09/2037
AC Camerfirma	2.047 bits	sha1WithRSAEncryption	2.003	14/11/2033
RACER	2.047 bits	sha1WithRSAEncryption	2.003	04/12/2023

Further information at https://www.camerfirma.com/politicas-de-certificacion-ac-camerfirma/

Reference documents:

- CONF-00-2012-01 ACTAS de ceremonias de creación de claves.

- CONF-00-2012-02/04 SCRIPTS de Generación de claves.
- CONF-00-2012-05 Informe Auditores.
- CONF-00-2012-03 Reparto de claves entre operadores.

6.1.1.1 CREATING THE SIGNATORY'S KEY PAIR

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

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

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

Keys are created using the RSA public key algorithm.

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

In a cloud management system, whether qualified or unqualified, keys are generated and stored in a signature creation device that conforms at least to the requirements in Annex II of the eIDAS Regulation.

The keys have a minimum length of 2048 bits.

6.1.1.2 KEY CREATION HARDWARE/SOFTWARE

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

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

6.1.2 PRIVATE KEY DELIVERY TO SUBSCRIBER

See section 3.2.1.

6.1.3 PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER

The public key is sent to Camerfirma to create the certificate when the circuit so requires. It is sent

in standard PKCS #10 format.

6.1.4 CA PUBLIC KEY DELIVERY TO RELYING PARTIES

The CA's certificate and fingerprint will be available to users on Camerfirma's web site https://www.camerfirma.com/ayuda/utilidades/descarga-de-claves-publicas/.

6.1.5 KEY SIZES

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

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

6.1.6 PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING

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

- Key size = minimum 2,048 bits.
- Key creation algorithm: rsagen1.
- Padding scheme: emsa-pkcs1-v1_5.
- Hash functions: SHA-256, SHA-512.

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

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

Root CA Private Keys MUST NOT be used to sign Certificates except in the following cases:

1) Self-signed Certificates to represent the Root CA;
2) Certificates for Subordinate CAs and Cross Certificates;
3) Certificates for OCSP Response verification.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 CRYPTOGRAPHIC MODULE STANDARDS AND CONTROLS

6.2.1.1 *THE CA'S PRIVATE KEY*

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

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

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

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

Subordinate CAs' keys are kept on devices that comply with at least FIPS 140-2 Level 3.

- CONF-2016-04-02 - Protección y activación de claves de CA Online.
- CONF-2012-04-10 - Script Ceremonia de emisión de certificados.

6.2.1.2 *THE SIGNATORY'S PRIVATE KEY*

The Signatory's private key can be stored in a software or SmartCard/Token device

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

In a cloud management system, whether qualified or unqualified, keys are generated and stored in a signature creation device that conforms at least to the requirements in Annex II of the eIDAS Regulation.

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

Camerfirma verifies over time that the QSCD devices used (SmartCard/Token and Cloud) continue to be certified in compliance with the requirements established in the eIDAS regulation, and that the national supervisory body continues to confirm that the operation of the Cloud QSCD devices by Camerfirma complies with the requirements established in the eIDAS regulation. In the event that the national supervisory body revokes the confirmation as QSCD of any of these devices, Camerfirma shall revoke the current certificates issued using said device.

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

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

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

Reference document: CONF-00-2012-03-Reparto de claves entre operadores.

6.2.3 PRIVATE KEY ESCROW

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

Exceptions:

- In case of certificates for information encryption Camefirma saves a copy of said key.
- In a cloud management system, whether qualified or unqualified, keys are generated and stored in a signature creation device that conforms at least to the requirements in Annex II of the eIDAS Regulation.

6.2.4 PRIVATE KEY BACKUP

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

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

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

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

In a cloud key management system, qualified or unqualified, the signer's keys can be backed up under the terms established by the corresponding regulations.

Camerfirma keeps records on CA private key management processes.

Reference document: CONF-00-2012-01-Acta de backup de las claves de las CA root.

6.2.5 PRIVATE KEY ARCHIVAL

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

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

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

When PKCS #12 format is used, Camerfirma ensure the elimination of user keys by executing a daily

task. This task verifies that three business days have not passed from the date of generation of the certificate. The folder where the files are stored has a filter that prevents files with extension p12 being backed up.

Camerfirma keeps records on CA private key management processes.

6.2.6 PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE

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

Reference document: CONF-00-2012-01/06/07/08 ACTAS de ceremonias de creación de claves.

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

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

In a cloud key management system, qualified or unqualified, as described in the device manufacturer's manual.

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

Keys associated with Signatories cannot be transferred.

Camerfirma keeps records on CA private key management processes.

6.2.7 PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE

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

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

In a centralized key management system, qualified or unqualified, as stated in the description in the device manufacturer's manual.

6.2.8 METHOD OF ACTIVATING PRIVATE KEY

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

The CA Root's key is activated via an m out of n process. See section 6.4.

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

In a centralized key management system , qualified or unqualified, as described in the description in the manufacturer's manual of the device provided to the subscriber after identity validation or by request at https://www.camerfirma.com/contacto-soporte/

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

Camerfirma keeps records on CA private key management processes.

6.2.9 METHOD OF DEACTIVATING PRIVATE KEY

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

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

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

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

In a centralized key management system , qualified or unqualified, as described in the description in the manufacturer's manual of the device provided to the subscriber after identity validation or by request at https://www.camerfirma.com/contacto-soporte/

6.2.10 METHOD OF DESTROYING PRIVATE KEY

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

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

Backups are destroyed securely.

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

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

In a cloud management system , qualified or unqualified, as described in the description in the manufacturer's manual of the device provided to the subscriber after identity validation or by request at https://www.camerfirma.com/contacto-soporte/

Camerfirma keeps records on CA private key management processes.

6.2.11 CRYPTOGRAPHIC MODULE RATING

Cryptographic modules are certified FIPS-140-2 level 3 are managed by at least two operators in a model n of m. The teams are housed in secure environments. The cryptographic module that stores

the Root keys is managed inside an isolated and disconnected cryptographic room. The cryptographic modules that store the Intermediate CA keys are stored in secure environments within a CPD following ISO27001 regulations.

In a cloud management system, whether qualified or unqualified, keys are generated and stored in a signature creation device that conforms at least to the requirements in Annex II of the eIDAS Regulation.

Camerfirma SA device providers are required to report the loss of qualification of certified devices. However, Camerfirma reviews at least annually with the suppliers that the devices have not lost the qualification, and will also be checked in the list provided by the European Commission.

If the device loses its qualification, the affected customers will be notified so that if they generate a qualified signature, they must stop using the device. Camerfirma will offer an alternative solution to the client to continue generating qualified signature. In any case, the certificate included in the device that has lost the certification will be revoked.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 PUBLIC KEY ARCHIVAL

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

6.3.2 CERTIFICATE OPERATIONAL PERIODS AND KEY PAIR USAGE PERIODS

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

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

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

All certificates issued by Camerfirma are valid from the moment of signature until the expiration date. No certificate issued to a web server can exceed a validity period of 825 days.

6.4 ACTIVATION DATA

6.4.1 ACTIVATION DATA GENERATION AND INSTALLATION

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

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

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

In Third-party HSM device. Camerfirma homologates third party devices, although these have an independent management. The keys are generated in an independent ceremony and Camerfirma is given a request for issuance of certificate along with the minutes of the ceremony.

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

6.4.2 ACTIVATION DATA PROTECTION

The activation data is communicated to the subject through an independent channel to the PKI management platform. Camerfirma does not store this information in its database when it comes to certificates in software or SmartCard/Token format. We do not store them in the cloud platform, as they are known and kept by the holder. The data can be sent back to the subject upon prior request to the email associated with the certificate, and will be effective as long as the user has not made a change in them previously.

In a cloud system, qualified or unqualified, as described in the description in the manufacturer's manual of the device delivered to the holder after validation of his identity.

6.4.3 OTHER ASPECTS OF ACTIVATION DATA

No stipulation.

6.5 COMPUTER SECURITY CONTROLS

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

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

Computers used are initially configured with the appropriate security profiles by Camerfirma system

personnel, for the following aspects:

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

6.5.1 SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS

Each Camerfirma server includes the following functions:

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

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

6.5.2 COMPUTER SECURITY RATING

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

6.6 LIFE CYCLE TECHNICAL CONTROLS

When the cryptographic keys associated with a certificate are stored on a SmartCard/Token device, this is always a qualified signature creation device in compliance with Annex II of the eIDAS Regulation.

As regards SmartCard/Token devices:

1) SmartCard/Token devices are prepared and sealed by an external provider.
2) The external provider sends the device to the registration authorities to be delivered to the Signatory.
3) The Signatory or RA uses the device to generate the key pair and send the public key to the CA.
4) The CA sends a public key certificate to the Signatory or RA, which is entered into the device.
5) The device can be reused and can store several key pairs securely.
6) The device is owned by the Subject/Signatory.

With respect to the devices used in the cloud platform: The device that stores these keys is FIPS-104-2 level 3 or EAL4+ certified and authorized by the national supervisor 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.

In response to intrusion and vulnerability analyses, adaptations are made to systems and applications that may have security problems, and to security alerts received from managed security services contracted with third parties. The corresponding RFCs (Request for Changes) are sent so that security patches can be incorporated or the versions with problems updated.

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

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

Reference documents:

- IN-2006-05-02-Clausulas exigible a desarrolladores externos.
- IN-2006-03-04-Control de cambios a Sistemas y Software.

6.6.2 SECURITY MANAGEMENT CONTROLS

6.6.2.1 SECURITY MANAGEMENT

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

An annual training plan has been established for such purposes.

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

6.6.2.2 DATA AND ASSET CLASSIFICATION AND MANAGEMENT

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

Reference document: IN-2005-02-15-Clasificación e Inventario de Activos.

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

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

Reference document: IN-2005-02-04-Política de Seguridad.

6.6.2.3 MANAGEMENT PROCEDURES

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

Reference document: IN-2010-10-08 Gestión de incidencias

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

Reference document: IN-2005-02-07 Funciones y responsabilidad del personal.

6.6.2.4 TRATAMIENTO DE LOS SOPORTES Y SEGURIDAD

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

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

Reference documents:

- CONF-2006-01-04-Procedimiento de Registro de Entradas y Salidas de Soportes
- IN-2012-04-03-Procedimientos Operativos de Seguridad para el Bastionado de Sistemas.

6.6.2.5 SYSTEM PLANNING

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

Reference documents:

- IN-2010-10-10 Gestión de Configuración
- IN-2010-10-05 Gestión de la capacidad
- IN-2010-10-03 Gestión de la Disponibilidad
- IN-2010-10-01 Gestión del Nivel de Servicio
- IN-2010-10-00 Manual de Gestión de Servicios de TI
- IN-2010-10-13 Planificación de Nuevos Servicios

6.6.2.6 INCIDENT REPORTING AND RESPONSE

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

Reference document: IN-2010-10-08 Gestión de incidencias

6.6.2.7 OPERATING PROCEDURES AND RESPONSIBILITIES

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

Reference document: IN-2005-02-07 Funciones y responsabilidad del personal

6.6.2.8 ACCESS SYSTEM MANAGEMENT

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

Reference document: IN-2011-04-10 Control de accesos a red.

In particular:

Overall:

1) There are controls based on firewalls, antivirus and IDS with high availability.
2) Sensitive data is protected via cryptographic methods or strict identification access controls.
3) Camerfirma has established a documented procedure to process user registrations and cancellations and a detailed access policy in its security policy.
4) Camerfirma has implemented procedures to ensure tasks are undertaken by the roles policy.
5) Each person is assigned a role to carry out certification procedures.
6) Camerfirma employees are responsible for their actions by the confidentiality agreement signed with the company.

Creating the certificate:

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

Revocation management:

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

Revocation status:

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

6.6.2.9 *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

No stipulation.

6.7 NETWORK SECURITY CONTROLS

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

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

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

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

Reference document: IN-2011-04-10 Control de accesos a red.

6.8 TIME-STAMPING

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

Reference document: IN-2006-04-01-Sincronización de tiempos.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

Certificate profiles comply with RFC 5280.

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

The profile records for these certificates can be requested at https://www.camerfirma.com/contacto-soporte/ or by telephone +34 91 344 37 43.

7.1.1 VERSION NUMBER

Camerfirma issues X.509 certificates Version 3.

7.1.2 CERTIFICATE EXTENSIONS

Certificate extension documents are described in the profile files. The profile records can be requested at https://www.camerfirma.com/contacto-soporte/ or by telephone +34 91 344 37 43.

7.1.3 ALGORITHM OBJECT IDENTIFIERS

The signature algorithm object identifier would be:

- 1.2.840.113549.1.1.5 – sha1WithRSAEncryption
- 1.2.840.113549.1.1.11 – sha256WithRSAEncryption
- 1.2.840.113549.1.1.13 – sha512WithRSAEncryption

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

7.1.4 NAME FORMAT

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

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

- The full name of the Signatory person, certificate holder or represented, in separate fields, or indicating the algorithm that allows the separation automatically.

- Name of the legal entity, where applicable.
- Numbers of the corresponding identification documents, by the law applicable to the Signatory person, certificate holder or represented, whether a natural person or a legal entity.

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

The exact semantics of the names described in the profile files. The profile records can be requested at https://www.camerfirma.com/contacto-soporte/ or by telephone +34 91 344 37 43.

7.1.5 NAME CONSTRAINTS

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

7.1.6 CERTIFICATION POLICY OBJECT IDENTIFIER

All 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

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

7.1.8 POLICY QUALIFIERS SYNTAX AND SEMANTICS

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

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

The CRL's detailed profile can be requested at https://www.camerfirma.com/contacto-soporte/ or by telephone +34 91 344 37 43.

7.2.1 VERSION NUMBER

The CRLs issued by Camerfirma are version 2.

7.2.2 CRL AND CRL ENTRY EXTENSIONS

Those established in the certification policies. The detailed profile of the CRL and its extensions can be requested at https://www.camerfirma.com/contacto-soporte/ or by telephone +34 91 344 37 43.

7.3 OCSP PROFILE

The profile for the OCSP messages issued conform to the specifications contained in the IETF RFC 6960.

In the OCSP responses the value of the nextUpdate field will be 23:59:59 hours after the answer, that is, the thisUpdate field.

7.3.1 VERSION NUMBER

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

7.3.2 OCSP EXTENSIONS

The profile of the OCSP responder certificates can be obtained at https://www.camerfirma.com/contacto-soporte/ or by telephone +34 91 344 37 43.

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

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

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

Camerfirma's objectives in relation to security and quality have essentially involved obtaining ISO/IEC 27001, ISO/IEC 20000, ISO 9001 and ISO 22301 certification and carrying out biennial audits on its certification system, and essentially on the Registration Authorities, in order to guarantee compliance with internal procedures.

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

(Applies only to Camerfirma Perú) Annually, the records, files, procedures and controls are reviewed as part of the audit lead by the Competent Administrative Authority (INDECOPI), according to the INDECOPI EC Accreditation Guidelines.

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

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

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

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

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

- ISO 27001, ISO 20000, ISO 9001 and ISO 22301 auditing on a three-year cycle with annual reviews
- eIDAS Conformity Assessment, biennial with annual review according to eIDAS Regulation to the following services:
    - *Qualified electronic time stamp*: ETSI EN 319 401, ETSI EN 319 421, ETSI EN 319 422
    - *Qualified certificate for electronic signature* (eIDAS Regulation art. 28): ETSI EN 319 401, ETSI EN 319 411-1 e 411-2, ETSI EN 319 412 (1,2,5)
    - *Qualified certificate for electronic seal* (eIDAS Regulation art. 38): ETSI EN 319 401, ETSI EN 319 411-1 e 411-2, ETSI EN 319 412 (1,2,3,5)
- Spanish/UE Personal Data Protection Act audit, biennial with annual review.

- Vulnerability audit quarterly.
- Penetration test yearly.
- RA audits on a discretionary basis.
- External TSUs on a discretionary basis.
- (Applies only to Camerfirma Perú) Additionally, for services provided in Perú from Camerfirma Perú Certificates - 2016, annual follow-up audits scheduled by INDECOPI and a renewal accreditation audit are carried out every 5 years.

8.1.1 EXTERNAL SUBORDINATE CA AUDITS OR CROSS-CERTIFICATION

Through its auditors, Camerfirma conducts an annual audit on the organizations that have obtained a Subordinate CA or TSA certificate and that issue certificates with their own technical and operational resources. It can also be replaced by a favorable report of the corresponding ETSI regulations such as ETSI EN 319 411-1.

8.1.2 AUDITING THE REGISTRATION AUTHORITIES

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

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

Reference documents:

- IN-2010-04-12-Procedimiento de Evaluación de la Seguridad en RA.
- IN-2010-04-15-Ficha de la visita de evaluación.
- IN-2010-04-16-Lista de Chequeo.
- IN-2006-03-08-Procedimiento Labores de RA.
- IN-2010-04-17-Informe de evaluación.

8.1.3 SELF-AUDITS

Annually Camerfirma performs internal audits (technical and legal control).

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

Audits are conducted by independent external companies that are widely renowned in computer

security, information systems security and in compliance audits by Certification Authorities:

- For ISO27001/20000 ISO 9001 audits - CSQA. https://www.csqa.it
- For ISO 14001 audit - CAMARA CERTIFICA. https://www.camaracertifica.es
- For conformity assessment of eIDAS Natural Person & Legal Person - CSQA. https://www.csqa.it
- For conformity assessment of eIDAS Timestamps - CSQA. https://www.csqa.it
- For internal audits / RA / Subordinate CA, TSA and Spanish Personal Data Protection Act - AUREN https://www.auren.com
- For the follow-up and renewal evaluations of CE and RE in Perú, the Auditor must be authorized by INDECOPI, and not have carried out work for it within the 2 years prior to the execution of the audit.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The audit companies used are independent and reputed companies with specialist IT audit departments that manage digital certificates and trusted services, which rules out any conflict of interest that may affect their activities in relation to the CA.

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

8.4 TOPICS COVERED BY ASSESSMENT

In general terms, the audits verify:

1) That Camerfirma has a system that guarantees service quality.
2) That Camerfirma complies with the requirements of the Certification Policies that regulate the issuing of the different digital certificates in the eIDAS Regulation (UE) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014.
3) That Camerfirma Perú complies with Peruvian regulation and INDECOPI Guidelines.
4) That the CPS is in keeping with the provisions of the Policies, with that agreed by the Authority that approves the Policy and as established under current law.
5) That Camerfirma properly manages the security of its information systems.

In general, the elements audited are:

- Camerfirma processes, Ras and related elements in the issuing of TSA timestamp certificates and OCSP validation services.
- Information systems.
- Protecting the data processing center.

- Documentation required for each type of certificate.
- Verification that the RA operators know Camerfirma's CPS and PCs.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

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

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

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

8.6 COMMUNICATION OF RESULTS

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

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 CERTIFICATE ISSUANCE OR RENEWAL FEES

The prices for certification services or any other related services are available and updated on Camerfirma's website https://www.camerfirma.com/certificados-digitales/ or by prior consultation with the Camerfirma support department at https://www.camerfirma.com/contacto-soporte/ or by telephone +34 91 344 37 43.

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

(Applies only to Camerfirma Perú) The prices of the issuance services (and where appropriate re-issuance) of Camerfirma Perú certificates are indicated by the Registration Entities, either on their respective web pages or by contacting by phone or mail.

9.1.2 CERTIFICATE ACCESS FEES

Access to certificates is free-of-charge, although Camerfirma applies controls in order to avoid mass certificate downloads. Any other situation that Camerfirma deems must be considered in this respect will be published on Camerfirma's website https://www.camerfirma.com/ or by prior consultation with the Camerfirma support department at https://www.camerfirma.com/contacto-soporte/ or by telephone +34 91 344 37 43.

9.1.3 REVOCATION OR STATUS INFORMATION ACCESS FEES

Camerfirma provides free access to information relating to the status of certificates or revoked certificates via certificate revocation lists or via its website https://www.camerfirma.com/ayuda/utilidades/validacion-de-certificados/.

Camerfirma offers the OCSP service free-of-charge. https://www.camerfirma.com/servicios-y-soluciones/respondedor-ocsp/.

9.1.4 FEES FOR OTHER SERVICES

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

9.1.5 REFUND POLICY

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

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

(Applies only to Camerfirma Perú): The rate reimbursement policy is included in the contracts subscribed by the Holder and Subscriber.

9.2 FINANCIAL RESPONSIBILITY

9.2.1 INSURANCE COVERAGE

Camerfirma, in its role as a CSP, has a public liability insurance policy that covers its liabilities to pay compensation for damages and losses caused to the users of its services: the Subject/Signatory and the User Party and third parties, for a minimum amount of 1,500,000 euros plus 500,000 euros for each eIDAS qualified service.

Said insurance must also cover the services provided by Camerfirma's subsidiaries abroad, considering as a subsidiary the ownership by AC Camerfirma, S.A. of more than 50% of the voting shares or participations.

9.2.2 OTHER ASSETS

No stipulation.

9.2.3 INSURANCE OR WARRANTY COVERAGE FOR END-ENTITIES

See section 9.2.1.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 SCOPE OF BUSINESS INFORMATION

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

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

Reference documents:

- IN-2005-02-04-Política de Seguridad.
- IN-2006-02-03-Normativa Seguridad.

9.3.2 INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION

Camerfirma considers the following information not confidential:

1) The contents of this CPS and the CPs.
2) The information contained in the certificates.
3) Any information whose accessibility is prohibited by current law.

9.3.3 RESPONSIBILITY TO PROTECT CONFIDENTIAL INFORMATION

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

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

9.3.3.1 DISCLOSURE OF INFORMATION ABOUT CERTIFICATE REVOCATION/SUSPENSION

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

Camerfirma provides a CRL and Certificate query service on the following website: https://www.camerfirma.com/ayuda/utilidades/validacion-de-certificados/

Camerfirma has an online query service for the status of certificates based on the OCSP standard at https://ocsp.camerfirma.com. The OCSP service provides standardized responses under RFC 2560 about the status of a digital certificate, i.e., whether the queried certificate is active, revoked or whether it has been issued or not by the certificate authority.

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

9.3.3.2 SENDING INFORMATION TO THE COMPETENT AUTHORITY

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

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 PRIVACY PLAN

In any case, Camerfirma complies with current regulations regarding data protection, in particular, it has adapted its procedures to the REGULATION (EU) 2016/679 General of Data Protection (RGPD). In this sense, this document serves, by 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.

Reference document: IN-2006-05-11-Conformidad de Requerimientos legales.

9.4.2 INFORMATION TREATED AS PRIVATE

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

9.4.3 INFORMATION NOT DEEMED PRIVATE

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

9.4.4 RESPONSIBILITY TO PROTECT PRIVATE INFORMATION

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

9.4.5 NOTICE AND CONSENT TO USE PRIVATE INFORMATION

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

9.4.6 DISCLOSURE PURSUANT TO JUDICIAL OR ADMINISTRATIVE PROCESS

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

9.4.7 OTHER INFORMATION DISCLOSURE CIRCUMSTANCES

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

9.5 INTELLECTUAL PROPERTY RIGHTS

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

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 CA REPRESENTATIONS AND WARRANTIES

9.6.1.1 CA

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

- Adhere to the provisions within the scope of this CPS and the corresponding Certification Policies.
- Protect its private keys and keep them secure.
- Issue certificates by this CPS, the Certification Policies and the applicable technical standards.
- Issue certificates by the information in its possession and which do not contain errors.
- Issue certificates with the minimum content defined by current law for qualified or recognized certificates.
- Publish issued certificates in a directory, respecting all legal provisions regarding data protection.
- Suspend and revoke certificates by this Policy and publish the revocations in the CRL.
- Inform Subjects/Signatories about the revocation or suspension of their certificates, on time and by current law.
- Publish this CPS and the Certification Policies on its website.
- Report changes to this CPS and the Certification Policies to the Subjects/Signatories and its associated RAs.
- Do not store or copy the Subject/Signatory's signature creation data except for encryption certificates and when it is legally provided for or allowed to be stored or copied.

- Protect data used to create the signature while in its safekeeping, if applicable.
- Establish data creation and custody systems in the aforementioned activities, protecting data from being lost, destroyed or forged.
- Keep data relating to the issued certificate for the minimum period required by current law.
- For certificates issued in centralized devices, qualified or unqualified, keep the private keys of the certificates, which can only be accessed by the Subjects/Holders, with due diligence.

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 paragraph 2, trust service providers shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under this Regulation.

  The burden of proving intention or negligence of a non-qualified trust service provider shall lie with the natural or legal person claiming the damage referred to in the first subparagraph.

  The intention or negligence of a qualified trust service provider shall be presumed unless that qualified trust service provider proves that the damage referred to in the first subparagraph occurred without the intention or negligence of that qualified trust service provider.

  2. Where trust service providers duly inform their customers in advance of the limitations on the use of the services they provide and where those limitations are recognisable to third parties, trust service providers shall not be liable for damages arising from the use of services exceeding the indicated limitations.

  3. Paragraphs 1 and 2 shall be applied in accordance with national rules on liability."

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

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 suspension and revocation of the certificates. Specifically, Camerfirma is fundamentally responsible for:

- The accuracy of the information contained in the certificate on the date of issue by confirming the applicant's details and the RA practices.
- Guaranteeing that when the certificate is delivered, the Subject/Signatory is in possession of the private key relating to the public key given or identified in the certificate when required, by using standard request forms in PKCS #10 format.

- Guaranteeing that the public and private keys work in conjunction with each other, using certified cryptographic devices and mechanisms.
- That the certificate requested and the certificate delivered match.
- Any liability established under current law.

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

9.6.1.2 *EXTERNAL SUBORDINATE CA*

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

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

Responsibility of the Subordinate CA (Internal/External):

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

9.6.2 RA REPRESENTATIONS AND WARRANTIES

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

- Adhere to the provisions of this CPS and the Certification Policy.
- Protect their private keys that are used for exercising their functions.
- Check the identity of the Subjects/Signatories and Applicants of certificates when necessary, definitively proving the Signatory's identity, for individual certificates, or the key holder, for

organization certificates, pursuant to the provisions of the corresponding sections of this document.

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

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

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

The RAs' responsibility:

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

1) Obligations prior to issuing a certificate.
   - Informing applicants about signing their obligations and responsibilities.
   - Properly identifying applicants, who must be trained or authorised to request a digital certificate.
   - Checking the validity of the applicant's details and the Entity's details, if there is a contractual relationship or powers of representation.
   - Accessing the Registration Authority application to process requests and issued certificates.
2) Obligations once the certificate has been issued.
   - Signing Digital Certification Service Provision agreements with applicants. In most issuance

processes, this contract is formalized by accepting the conditions on the websites that are part of the process of issuing the certificate. The certificate cannot be issued without the terms of use having previously been accepted.

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

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

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

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

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

9.6.3 SUBSCRIBER REPRESENTATIONS AND WARRANTIES

9.6.3.1 SIGNATORY/CREATOR OF THE SEAL

The Signatory/Creator of the seal (either directly or through an authorized third party or "Applicant") 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.
- Use the information of the signatory under the rules imposed by the Data Protection law.
- Allow the publication of digital certificates in a public repository.
- To provide the RA with the necessary information to carry out a correct identification.
- Guarantee the accuracy and veracity of the information provided.

- Notify any change in the data provided for the creation of the certificate during its period of validity.
- Custody of your private key activation data in a diligent manner. You will be solely responsible to third parties or to the entity you represent if you are not authorized to do so, for the consequences that an improper use or not properly controlled may generate.

9.6.3.2 SUBJECT/HOLDER

The subject will be obliged to comply with the provisions of the regulations in force and in addition to:

- Use the certificate as established in the present CPS and in the applicable Certification Policies.
- Respect the provisions of the documents signed with Camerfirma and the RA.
- Inform as soon as possible of the existence of any cause for suspension / revocation.
- Notify 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 Camerfirma or the RA of the suspension or revocation of the same one, or once the term of validity of the certificate has expired.
- To make use of the digital certificate with the character of personal and non-transferable and to guard the data of activation of the private key of diligent way, therefore, to assume the responsibility for any action that is carried out in contravention of this obligation, as well as to fulfil the obligations that are specific of the applicable norm to the above mentioned digital certifications. It may be held liable to third parties or to the entity it represents, if it is not authorised to do so, for the consequences that improper use or improperly controlled use may generate.
- To authorize Camerfirma 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 relevant certification service provider 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 SmartCard/Token device, in the event that it loses its possession, make it known to the entity that issued it 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 given by the corresponding certification service provider to carry out any transaction prohibited by the applicable law.

In the case of qualified certificates, the Signatory or certificate holder must use the key pair exclusively for the creation of electronic signatures or seals and by any other limitations notified to it.

You should also be especially diligent in the safekeeping of your private key and your qualified signature-creation device, in order to avoid unauthorized use.

If the Signatory generates its own keys, it undertakes to:

- Generate its Signatory keys using an algorithm recognized as acceptable for the electronic signature, in its qualified case, or the electronic seal, in its qualified case.
- Create the keys within the signature or seal creation device, using a qualified device where appropriate.
- Use lengths and key algorithms recognized as acceptable for the electronic signature, where appropriate qualified, or the electronic seal, where appropriate qualified.

9.6.3.3 ENTITY

In the case of those certificates that imply a link to an Entity, the Entity will be obliged to request to the RA the suspension/revocation of the certificate when the Subject/Signer ceases to be linked to the organization.

9.6.4 RELYING PARTY REPRESENTATIONS AND WARRANTIES

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

- Verify the validity of the certificates before performing any operation based on them. Camerfirma has several mechanisms to perform such verification as access to lists of revoked or online consultation services such as OCSP, all these mechanisms are described on the website of Camerfirma. In particular, to ensure that it is before a qualified certificate must perform the validation against the TSL in force at all times.
- 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 the case of Legal Person Representative certificates (or entity without legal personality) for Proxies that involve a representation relationship based on a special power of attorney or private document with limited faculties, third parties should check the limits of such faculties.

- Verify the validity of the qualification of a signature associated with a certificate issued by Camerfirma by verifying that the certification authority that has issued the certificate is published in the trust list of the corresponding national supervisor.

9.6.5 REPRESENTATIONS AND WARRANTIES OF OTHER PARTICIPANTS

No stipulation.

9.7 DISCLAIMERS OF WARRANTIES

By current law, the responsibility assumed by Camerfirma and the RA does not apply in cases in which certificate misuse is caused by actions attributable to the Subject and the User Party due to:

- Not having provided the right information, initially or later as a result of changes to the circumstances described in the digital certificate, when the certification service provider has not been able to detect the inaccuracy of the data;
- Having acted negligently in terms of storing the data used to create the signature and keeping it confidential;
- Not having requested the suspension or revocation of the digital certificate data in the event of doubts raised over their storage or confidentiality;
- Having used the signature once the digital certificate has expired;
- Exceeding the limits established in the digital certificate.
- Actions attributable to the User Party, if this party acts negligently, that is, when it does not check or heed the restrictions established in the certificate in relation to allowed use and limited number of transactions, or when it does not consider the certificate's validity situation.
- Damages caused to the Subject or trusting third parties due to the inaccuracy of the data contained in the digital certificate, if this has been proven via a public document registered in a public register, if required.
- An inadequate or fraudulent use of the certificate in case the Subject / Holder has assigned it or authorized its use in favour of a third person by virtue of a legal transaction such as the mandate or empowerment, being the sole responsibility of the Subject / Holder the control of the keys associated with your certificate.

Camerfirma and the RAs are not liable in any way in the event of any of the following circumstances:

- Warfare, natural disasters or any other case of Force Majeure.
- The use of certificates in breach of current law and the Certification Policies.
- Improper or fraudulent use of certificates or CRLs issued by the CA.
- Use of the information contained in the Certificate or CRL.

- Damages caused during verification of the causes for revocation/suspension.
- Due to the content of messages or documents signed or encrypted digitally.
- Failure to retrieve encrypted documents with the Subject's public key.

9.8 LIMITATIONS OF LIABILITY

(Doesn't apply to CA Peru) The monetary limit of the transaction value is expressed in the final entity's certificate by including the extension "qcStatements", (OID 1.3.6.1.5.5.7.1.3),. The monetary value expression shall be in keeping with section 4.3.2 of standard ETSI EN 319 412-05.

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

9.9 INDEMNITIES

See section 9.2 and 9.6.1.

9.10 TERM AND TERMINATION

9.10.1 TERM

See section 5.8.

9.10.2 TERMINATION

See section 5.8.

9.10.3 EFFECT OF TERMINATION AND SURVIVAL

See section 5.8.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

Any notification in relation to this CPS shall be made by email or certified mail to any of the addresses listed in the contact details section 1.5.2.

9.12 AMENDMENTS

9.12.1 PROCEDURE FOR AMENDMENT

The CA reserves the right to modify this document for technical reasons or to reflect any changes in the procedures that have occurred due to legal, regulatory requirements (eIDAS, CA/B Forum, National Supervisory Bodies, etc.) or as a result of the optimization of the work cycle. Each new version of this CPS replaces all previous versions, which remain, however, applicable to the certificates issued while those versions were in force and until the first expiration date of those certificates. At least one annual update will be published. These updates will be reflected in the version box at the beginning of the document.

Changes that can be made to this CPS do not require notification except that it directly affects the rights of the subscriber, in which case they may submit their comments to the organization's policy administration within 15 days following the publication.

9.12.2 NOTIFICATION MECHANISM AND PERIOD

9.12.2.1 LIST OF ASPECTS

Any aspect of this CPS can be changed without notice.

9.12.2.2 NOTIFICATION METHOD

Any proposed changes to this policy are published immediately on Camerfirma's website https://www.camerfirma.com/practicas-de-certificacion-ac-camerfirma-cps-dpc/

For Perú: https://www.camerfirma.com.pe/normativa/

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. Especially the changes in this CPS will be notified to the National Supervision Bodies:

- Spain: National supervisor body.
- Perú: INDECOPI.
- Colombia: ONAC.
- México: UFE.

9.12.2.3 PERIOD FOR COMMENTS

The affected Subjects/Signatories and Trusted Third Parties can submit their comments to the policy management organization within 15 days following receipt of notice.

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

No stipulation.

9.13 DISPUTE RESOLUTION PROCEDURE

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

9.14 GOVERNING LAW

The execution, interpretation, modification or validity of this 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 Signers and third parties that rely on the Certificates assume in their entirety the content of this Certification Practices and Policy Statement.

9.16.2 ASSIGNMENT

Parties to this CPS may not assign any of their rights or obligations under this CPS or applicable agreements without the written consent of Camerfirma.

9.16.3 SEVERABILITY

Should 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.

9.16.5 FORCE MAJEURE

Force Majeure clauses, if existing, are included in the “Subscriber Agreement”.

9.17 OTHER PROVISIONS

No stipulation.

Apendice 1 Document history

May 2016	V1.0	eIDAS adaptation
Nov 2016	V1.1	Modifications made to the conformity evaluation process.
Mar 2017	V1.2	Expansion of CA structures, reviewing and modifying certificate profiles.
Apr 2017	V1.2.1	Incorporation of CAA checks into Secure Server and Digital Office certificates pursuant to RFC 6844.
Feb 2018	V1.2.2	1.2 clarification on the alignment of these practices with the Baseline Requirements of CA-B FORUM (point 1.1 after adaptation to structure RFC3647) 1.2.1.3 - OIDs corrections of EP certificates with PSEUDÓNIMO (point 1.3.11.3 after adaptation to structure RFC3647) 1.2.1.3.4 - Clarification of the duration of the TSU certificates and acceptance of the practices by the subscriber with an approved TSU device. (point 1.3.11.3.4 after adaptation to structure RFC3647) 1.2.1.4.3 - Incorporation of the date of deployment of Camerfirma Perú (point 1.3.11.4.1.7 after adaptation to structure RFC3647) 1.5.5 - Incorporation of the figure of Delegate Agency for Camerfirma Perú (point 1.3.2 after adaptation to structure RFC3647) 4.8.3 Revocation by third parties. Revocation in case of an incorrect issuance (CABFORUM requirement). (point 4.9.2 after adaptation to structure RFC3647)
Mar 2018	V1.2.3	1.5.5 RAs for SSL can't validate the domain. CA / B Forum. (point 1.3.2 after adaptation to structure RFC3647) 2.5.3 Clarification free service OCSP. (point 9.1.3 after adaptation to structure RFC3647) 2.1.5 user responsibility - TSL check (point 9.6.4 after adaptation to structure RFC3647)
May 2018	V1.2.4	1.3.3, 1.3.9 y 1.3.10 Clarifications concepts Subject / Holder and Signer / Creator of the seal. 3.2.3.1 Other documents accepted to prove the link between the owner of the domain and the certificate holder. 9.1.5 Political modification of withdrawals 9.4 Update of the privacy clause of personal information according to RGPD 9.7 Exemption of responsibility of the CA and AR in case of delegation

		of the certificate to a third party Adaptation of the structure of the CPD document based on RFC3647 1.3.11.3 Incorporation of hierarchy CHAMBERS OF COMMERCE ROOT - 2018 1.3.11.4 Incorporation of subordinated CA AC CAMERFIRMA GLOBAL TSA – 2018
Jun 2018	V1.2.5	Nomenclature correction from safe device to qualified device. Correction of URLs by changing Camerfirma website. Incorporation of CA CN = Camerfirma Corporate Server II - 2015 as qualified CA. 3.2.1 Storage of keys generated by Camerfirma and stored remotely. 3.2.3.2 Corrections. 3.2.3.4 Eliminated 3.2.3.4 Considerations in the identification of users and linkage in the AAPP. 3.3.2 Incorporation of additional explanatory text. 4.1.2.5 Modification cross-certification. 8.1.1 Correction requirements for organizations with certificates of Intermediate CA or Camerfirma cross-certification. 8.2 Update eIDAS auditors.
Jul 2018	V1.2.6	1.3.11.4.1.4 qualifying TSU certificates validity's is 5 years maximum 8.7 Self-Audit about 3% of the Server Certificates. 9.12.2.2 Nacional supervisor body notification ES, PE, CO, MX Change of order, denomination and development in different points to meet RFC3647 Point '9.12.1 Procedure for amendment' is developed
Sep 2018	V1.2.7	Change of order, denomination and development in different points to meet RFC3647 Point '9.12.1 Procedure for amendment' is developed
Sep 2018	V1.2.8	3.2.5.1 Proof of relationship, the domain validation will be done by one of the methods accepted by CA/B Forum Declaration of the Guidelines for The Issue And Management Of Extended Validation Certificates version prepared by the CA/B Forum with which these CPS are aligned.
Sep 2018	V1.2.9	minor changes to the document format

		3.2.5.1 Identification of the link. Explicit statement of the methods used. 3.2.3 Incorporation of the control check procedure on the applicant's email account. 4.2.1 Included are the AAC checks previously stated in 3.2.5.2. Hierarchy withdrawn CHAMBERS OF COMMERCE ROOT - 2018 9.16.4 updated 6.2.3 updated
Feb 2019	V1.2.10	1.3.2 Modification and clarification of the concept of Delegated Agency in the CA Camerfirma Perú and it is withdrawn that the Spanish Companies can be RAs of the CAs: AC CAMERFIRMA FOR WEBSITES-2016, AC CAMERFIRMA GLOBAL FOR WEBSITES-2016 and CAMERFIRMA CORPORATE SERVER II - 2015. 1.3.2 Includes CHAMBERS OF COMMERCE ROOT 2018 hierarchy 1.3.5.7.3.1 the 2016 hierarchy is replaced by the 2018 hierarchy 1.3.5.7.3.5 AC CAMERFIRMA FOR NATURAL PERSONS. (Certificates for natural persons) 1.4.1 Appropriate uses of certificates 1.4.2 Prohibited and Unauthorized Uses of Certificates 1.6.2 Definition of Remote Signature and Remote Seal 2.2.1 Certification Policies and Practices. 2.2.2 Terms and Conditions. 3.1.3 Remove reference to policies. 3.1.5.1 Issuance of several physical person certificates for the same holder. 3.1.6 Recognition, authentication and function of trademarks and other distinctive signs 3.2.1 Methods of testing private key ownership and reference to QSCD list. 3.2.2.1 Identity 3.2.3 Identification of an individual's identity. 3.2.2.5 IP URL record 3.4 Identification and authentication of a revocation request 4.1.2.4 elimination reference policies

		4.1.2.5 Cross certification notes 4.2.2 clarification delivery documentation and WS access 4.2.3 Unspecified Sub-CA period 4..3.1.3 Authenticated WS Requests. 4.5.1 Use of the certificate and the subscriber's private key, including conditions of use for remote signature and remote seal. 4.5.1 Includes CHAMBERS OF COMMERCE ROOT 2018 hierarchy 4.6.1 No component certificate renewals. 4.9.2 Remove reference to policies. 4.9.5 Clarification revocation 4.12.1 Incorporation of key custody in a centralized device. 5.2.1 Remove policy reference 5.3.1 Delete reference document 5.5.1 Custody of events related to the centralized key management platform. 5.7 Delete reference document 5.7.4 Delete time reference 6.1.1 Includes CHAMBERS OF COMMERCE ROOT 2018 hierarchy 6.1.1.1 Include onbehalf treatment 6.2.1.2 Error in reference document go to 6.2.1.1 - Include Onbehalf 6.2.3 Include onbehalf treatment 6.2.4 Include onbehalf treatment 6.2.6 Include onbehalf treatment 6.2.7 Include onbehalf treatment 6.2.8 Include onbehalf treatment 6.2.9 Include onbehalf treatment 6.2.10 Include onbehalf treatment 6.2.11 Include onbehalf treatment 6.4 Activation of signature data on a centralized platform. 6.4.2 Include onbehalf treatment 6.6 Centralized platform life cycle management. 9.6.4 The responsibility of the Signatory/Creator of the seal and of the

		Subject/Holder in case of delegation of the use of certificates to third parties is warned. 9.6.5 Obligation and responsibility of third parties, the obligations of certificates of Representative of Legal Person are detailed 9.6.1.1 Incorporation of CA responsibility for centrally stored keys. 9.6.2 Obligation and responsibility of the RA 9.6.4.1 and 9.6.4.2 Clarifies the responsibility of the Subject/Holder and of the Signatory/Creator of the seal with respect to their obligations of custody of the data of activation of the private key. 9.7 Liability disclaimer 9.12.2.2 Communication of changes to auditors
Jan 2020	V1.2.11	1.3.1 Incorporates corporate data of AC Camerfirma SA and its participation by InfoCert, S.p.A. 1.3.2 Adding requirements for issuing certificates to non-residents in Spain and for authorization of external RAs that issue Secure Server certificates 1.3.5.1 Substitute throughout the document the term "SubCA" with "Intermediate CA" or "Subordinated CA" and its submission to the Root CA CPS 1.3.5.7 It is clarified that the CPS includes the hierarchies and CAs managed by Camerfirma as the owner. CAs owned by other organizations, are governed by their own CPS. 1.3.5.7.3 Update of the CHAMBERS OF COMMERCE Hierarchy: - revocation of CA Root "CHAMBERS OF COMMERCE ROOT 2018" and intermediate CA "AC CAMERFIRMA FOR WEBSITES 2018" - revocation of intermediate "AC CAMERFIRMA CODESIGN – 2016" (under CHAMBERS OF COMMERCE ROOT-2016") - creation of IVSIGN CA (own CPS under CHAMBERS OF COMMERCE ROOT -2016") 1.3.5.7.3.2 Clarify how keys are generated and stored 1.3.5.7.3.5.2.1 Clarifications of the functionalities of the Qualified Legal Representative Certificates, 1.3.5.7.4 Update of the GLOBAL CHAMBERSIGN ROOT Hierarchy - 2016: - revocation of intermediate CA "AC CAMERFIRMA – 2016" and all its second level intermediate CAs

		- revocation of the intermediate AC CITISEG - 2016 (under intermediate AC "AC CAMERFIRMA COLOMBIA – 2016") - creation of second level intermediate CAs "CAMERFIRMA COLOMBIA SAS CERTIFICATES – 001" and "CAMERFIRMA COLOMBIA SAS CERTIFICATES – 002" (under intermediate AC "AC CAMERFIRMA COLOMBIA – 2016") 2.3 CPS version periodicity is incorporated 3.2.2.1 In identifying the entity for SSL EV certificates, the entity category must be checked according to CA / Browser Forum policies 3.2.3 The alternative methods of identifying a natural person as set out in the eIDAS Regulation are detailed in art. 24.1 and it is indicated that the checking of the email control is done exclusively by the CA 4.5.1 The key usage table is updated with the current CAs 4.9 Where to check expired and non-expired certificates is required and for how long in case of intermediate CA revocation 4.9.1 Added 2 revocation causes aligned with Mozilla Root Store Policy 4.9.7 The CRL emission frequency table is updated with the current CAs 6.1.1 The table on key pair generation with current CAs is updated 6.1.7 It is explicitly stated that root keys do not issue end-entity certificates (except for OCSP responders) 6.2.11 Control of the qualification of devices and actions in case of loss 8.1.3 Clarification frequency internal audits and volume for SSL
May 2020	V1.2.12	1.3.2 where is said "domain possession" change to "domain control" 1.3.5.7.3 CHAMBER OF COMMERCE Hierarchy: incorporation of CHAMBERS OF COMMERCE ROOT and intermediate CA "AC CAMERFIRMA CERTIFICADOS CAMERALES" 1.3.5.7.3.3 Removal of information about Codesign certificates (AC CAMERFIRMA CODESIGN – 2016 has been revoked) 1.3.5.7.4 GLOBAL CHAMBERSIGN ROOT Hierarchy: incorporation of new OIDs from intermediate CA "AC CAMERFIRMA PERÚ CERTIFICADOS – PERÚ" issued in Hardware device (adaptation to EC v.4.1 INDECOPI Guide) 3.2.3 Authentication of individual identity: new writing to incorporate eIDAS and national methods of identification. 3.2.5.1 Added reference about preservation of information and documentation of data issuance in paper or electronical means.

		Domain ownership evidence is removed. 4.5.1 The key usage table is updated with the current CAs 4.9.7 The CRL emission frequency table is updated with the current CAs 5.2.1 It is specified that an RA Operator cannot issue a certificate to himself 6.1.1 The table on key pair generation with current CAs is updated 7.3 OCSP Message Profile Specifications Required 8.1 References to WebTrust Audits are removed and the ETSI standards on which the eIDAS audit is based are detailed. 8.2 The identification of audits and auditors is updated
Jan 2021	V1.2.13	1.3.5.7.3 and 1.3.7.5.4 Incorporation of OIDs
Feb 2021	V1.2.14	3.2.1.1 Registration Agencies incorporation. 4.3.1.4 ETSI TS 119 431-2 signature policy incorporation. 4.6.1 Change in the period of key use for a TSU certificate. 5.4.3 Audit log retention period updated.
Mar 2021	V1.2.15	1.1 (and the rest of the document) the reference to Law 59/2003 is eliminated and reference to Law 6/2020 is added. 1.3.5.7.7.3, 1.3.5.7.3.4.1.2, 1.3.5.7.3.4.1.3 With the same OID, new certificates of Self-Employed and Chartered Self-Employed are incorporated. 1.3.3.5.7.7.3.4.4.2 Clarifications on the powers of the Representatives and how to accredit them. 1.3.3.5.7.7.4.2.2.1 Clarifications on the name of the certificate profiles under the CA CAMERFIRMA PERU for their adaptation to the INDECOPI Guidelines. 1.4.1 and 1.4.2 Clarifications on appropriate uses of the certificates and prohibited uses 3.2.5.1 Addition of information on the 'Documentation' supporting the certificates of Self-Employed and Self-Employed Member of a Professional Association. 3.3.1 Clarification in the wording of validation for certificate renewal and compliance with Law 6/2020 Throughout the document: modification of the URLs that refer to the Camerfirma website after launching a new website with a change in the information structure.

Apr 2021	V1.2.16	1.3.5.7.4.2 Extension to LATAM of the geographical scope of the AC Camerfirma Perú 4.9.12 Inclusion of the instructions to notify private key compromise
Jul 2021	V1.2.17	(only in English version) 4.9.12 correction of the editing bug in sections 4.9.12 and 4.9.13 The withdrawal from this CPS of AC CAMERFIRMA FOR WEBSITES 2016 and CAMERFIRMA CORPORATE SERVER 2015 II and the requirements and details of the website certificates 1.3.5.7.3 Include CamerCloud profiles and OIDs 1.3.5.5.7.3.2.2 The point at which the different TSU certificates will be available is specified. 1.6.1 Addition of new acronyms 3.2.3 Extended information on VideoID and incorporation of SelfID 4.3.1.4 Addition of ManagedOnBehalf certificate requirements 4.4.3.1 addition of policy OID for certificates in non-certified signature creation or seal creation devices 6.2.8,6.2.9,6.2.10,6.4.2 Further detailed information for certificates in CKC.
Oct 2021	V1.2.18	1.1 General Overview: Include a generic presentation of Camerfirma Perú, S.A.C., references to the regulations that apply to Peruvian CA and the services provided under INDECOPI accreditations. It is reported that these CSP apply to AC Camerfirma Perú Certificates - 2016 unless it is expressly indicated that "Does not apply to CA Perú" or " Applies only to Camerfirma Perú". 1.3.1 Include the corporate and contact details of Camerfirma Perú, S.A.C. as a Certification Authority. 1.3.2 Include description of Registration Entity (ER) of Camerfirma Perú S.A.C. and external REs. Summary table is removed. 1.3.3 The definition of the "Holder" of the certificate is added according to Peruvian regulations. 1.3.5.2 Include a reference to the Competent Administrative Authority in Perú (INDECOPI) 1.3.5.4 The definition of the "Entity" role is added for electronic seal certificates. 1.3.5.5 Definitions of "Applicant" and "Subscriber" roles are added according to Peruvian regulations. 1.3.5.6 The definition of the "Responsible" of the certificate is added

		according to Peruvian regulations. 1.3.5.7.4. and 1.3.5.7.4.2 AC Camerfirma Perú Certificates - 2016. Modification of the denomination of several Peruvian profiles to adjust them to the denomination used in the Peruvian legal framework applicable to digital signature and certificates and the INDECOPI Guidelines. Incorporation of new profiles: Company electronic Seal in Panama and Natural Person Certificate - Registered Professional. 1.4.2 It is considered prohibited and unauthorized uses, the ones determined by Peruvian regulations. 1.6.1 Acronyms for CE and RE are added according Peruvian terminology. 1.6.2 Definitions of Certification Authority and Registration Authority are modified to incorporate Certification Entities and Registration Entities according to Peruvian terminology. 2.1 and 2.2 Add links to services on the Camerfirma Perú website. 3.1.1 The contact telephone number is modified and the reference to TSL certificates is eliminated. 3.2.2.1 It is added that the CA of Perú may use the Commercial Registry of Panama to identify the entities. 3.2.3 Reference is added to the identity documents of a national or resident individual in Perú. 3.3 Conceptual and terminological clarification applicable to CA Perú regarding the “re-issuance” of certificates. 4.5.1 New profiles are added in the certificate use box and the subscriber's private key. 4.6.1 Specific circumstances of the reissues of certificates under the CA Perú are added, although it is indicated that the service is not currently available. 4.6.7 Paragraph on TSL certificate is deleted. 5.7.1 It is specified that certificates will not be issued while CA private key compromise persists. 5.8 Actions are added in the event of CA or RA termination to include Peruvian requirements. 8. Throughout the section, a reference is added to the audits that apply to services provided in Perú. 9. It is specified where to find the rates and refund policy for the services provided in Perú.

		9.2.1 Modification of the amounts covered by the Insurance by Law 6/2020 and reference about subsidiaries services coverage.
Nov 2021	V1.2.19	1.3.5.2 The declaration of the national supervisory body within the Spanish State is updated. 1.3.5.7.3 The root 'Chambers of Commerce Root - 2008' is included. 1.3.5.5.7.3 Additional information about the devices where the keys are generated is incorporated. 1.3.5.5.7.3 Specified whether the OIDs of existing policies correspond to those generated and stored on QSCD Card/Token, QSCD Cloud or Non-QSCD devices (Software, Cloud or External Device). 1.3.5.7.3 The Timestamp certificates issued by Camerfirma AAPP II - 2014 are removed from this table. 1.3.3.5.7.7.3.1.1 A declaration is withdrawn and incorporated into point 1.3.5.7.3. 1.3.3.5.7.7.3.3.3 Incorporate clarification of the OIDs incorporated in the certificates issued in qualified and non-qualified devices. 3.2.1 Improvement in the information provided on the different methods of proof of private key possession. 3.2.3 Clarifications related to the methods of identification and incorporation of the reference into the assisted process with pre-validation of documentation. 3.3 Correction to the name of the CA. 4.1.2.1 Correction of the PKCS used and extended declaration. 4.3.1.4 Clarification of the OIDs embedded in the certificates is incorporated. 4.9.11 Replacement of the referenced web page. 4.12.1 Statement that they can be qualified and non-qualified devices. 4.12.1, 5.5.1, 6.2.4, 6.2.6, 6.2.7, 6.2.8, 6.2.9, 6.2.10, 6.4.2, 9.6.1.1 Replacement of the term CKC with 'qualified or unqualified'. 6.1.1.1 Rewording of the paragraph referring to CKCs. 6.2.1.2 More information is provided on generation in the centralized platform and the checks Camerfirma performs. 6.2.3 The exception for keys generated in centralized platforms managed by Camerfirma is included. 6.2.11 More information on generation in the centralized platform is added.

		9.12.2.2.2 Substitution of *Ministerio de Economía y Empresa* for National Supervisory Body.
2022-05-17	V1.2.20	The document format is updated and a document code is added. The possibility of generating keys on non-qualified devices (cards and tokens) is incorporated. The names of the qualified certificate profiles issued by the CAs appearing in this CPS are updated to better define their nature. All references to the STATUS platform are updated as Camerfirma STATUS®. 1.3.1 The content of point 1.3.5.1 of the previous version is incorporated. 1.3.5.7 its contents are moved to 1.3.1.1. 1.5 Content is updated. The term 'hardware' is replaced by 'Card/Token' where deemed necessary. 1.3.1.1.1.3.3.2.5 and 1.3.1.1.1.3.3.2.6 are updated in their wording. 1.3.3.5.7.3.3.2.2 TSU certificates are eliminated. 4.4.3 becomes not stipulated. 5.2.1 The incompatibility between the role of CA Administrator and CA Operator is eliminated. 5.4.3 The retention period of the audit logs is increased. 5.7 Its content is updated. 5.8 The content of the item is updated. 6.6.2 The distribution of the contents of the item is updated. Minor changes in the wording of the document. The data on the creation, verification and approval of this PSC is updated on the cover page of the document.
2022-07-15	V1.3.0	This document changes its name from "CERTIFICATION PRACTICE STATEMENT DIGITAL CERTIFICATES AC CAMERFIRMA SA EIDAS" to "CERTIFICATION PRACTICE STATEMENT CAMERFIRMA 2003-2008-2016". This document is a continuation of the document "'CERTIFICATION PRACTICE STATEMENT DIGITAL CERTIFICATES AC CAMERFIRMA SA EIDAS V1.2.20". Minor changes in the document's style and punctuation.

		1.1 Version update of the EN 319 401 reference version and additional content. 1.3.1 Certification Authorities. Overall changes. 3.2.3 Authentication of individual identity. More specificity in identification methods 2 and 3. 3.2.5.1 Proof of relationship. Incorporation of code signing certificates. 4.4.3, 4.10.3, 4.12.2, 5.3.5, 6.4.3, 6.3.3, 7.1.8, 9.2.2, 9.6.5, 9.12.3 and 9.17 - replace 'Not stipulated' with 'No stipulation'. 4.5.1 Subscriber private key and certificate usage. Incorporation of the cases added to point '1.3.1 Certification Authorities' in this version of this document. 4.9.3 Procedure for revocation request. Updating of procedures. 4.9.5 Time within which CA must process the revocation request. A 24-hour time limit is set between the receipt of the revocation request and the publication of the revocation. 4.9.7 CRL issuance frequency. Incorporation of the cases added to point '1.3.1 Certification Authorities' in this version of this document. 6.1.1 Key pair generation. Incorporation of the cases added to point '1.3.1 Certification Authorities' in this version of this document. 7.1.3 Algorithm object identifiers. Incorporation of the sha1WithRSAEncryption algorithm.
2022-08-23	V1.3.1	1.3.1.2 CHAMBERS OF COMMERCE ROOT HIERARCHIES, replacement of 'Certificado de TSU' with 'TSU Certificate'. 1.3.1.2, 3.2.5.1, 4.5.1, in 'AC CAMERFIRMA PERÚ CERTIFICADOS – 2016' replacement of 'Natural Person Certificate for Registered Professional' with 'Legal Person Certificate - Registered Professional Attribute' 1.3.1.2.2.1.8 Legal Person Certificate - Registered Professional Attribute, rewording of the text describing this profile. 1.3.2 REGISTRATION AUTHORITY (RA), replacement of 'Delegate Agency' by 'Subsidiary'. 1.6.1 ACRONYMS, 5.1.1 SITE LOCATION AND CONSTRUCTION, 5.1.2 PHYSICAL ACCESS, the OCSP service is provided from AWS cloud. 4.9.2 WHO CAN REQUEST REVOCATION, incorporating the possibility of requesting revocation through an electronic seal based on a certificate issued by Camerfirma on behalf of the Entity. 4.9.3 PROCEDURE FOR REVOCATION REQUEST, incorporation of

		revocation procedure through web service. 5.4.3 RETENTION PERIOD FOR AUDIT LOGS, reduction of the retention period from 20 to 15 years. Minor changes in the wording of the document. Appendix I: document history, incorporation of the signing date of this document in its version 1.3.0