



AN INFOCERT COMPANY

**CERTIFICATION
PRACTICE STATEMENT
AND
CERTIFICATE POLICIES
CAMERFIRMA**

Version 1.5.0

Drafting and Revision: Camerfirma Compliance and Legal Departments

Approved by (PA): Camerfirma Legal Department

Document valid only in digital format electronically signed or sealed by the Policy Authority (PA).

This document can be obtained from the website address

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

Language: English

Code: PUB-2022-18-04

INDEX

1 INTRODUCTION	12
1.1 OVERVIEW	12
1.2 DOCUMENT NAME AND IDENTIFICATION	16
1.3 PKI PARTICIPANTS	19
1.3.1 CERTIFICATION AUTHORITIES (CAS)	19
1.3.1.1 CHAMBERS OF COMMERCE ROOT hierarchies	20
1.3.1.2 GLOBAL CHAMBERSIGN ROOT hierarchies	37
1.3.1.3 CAMERFIRMA ROOT 2021 hierarchy	40
1.3.1.4 INFOCERT-CAMERFIRMA ROOT 2024 HIERARCHY	46
1.3.1.5 OCSP certificates	49
1.3.1.6 Test certificates	50
1.3.1.7 Internal management CA	50
1.3.2 REGISTRATION AUTHORITIES (RAS)	50
1.3.3 SUBSCRIBERS	52
1.3.3.1 Subscriber	52
1.3.3.2 Subject, Signatory and Creator of a Seal	53
1.3.3.3 Applicant	55
1.3.3.4 Person Responsible	56
1.3.3.5 Entity	56
1.3.4 RELYING PARTIES	57
1.3.5 OTHER PARTICIPANTS	57
1.3.5.1 Supervisory Body	57
1.3.5.2 Trust Service Provider (TSP) and Qualified Trust Service Provider (QTSP)	57
1.4 CERTIFICATE USAGE	58
1.4.1 APPROPRIATE CERTIFICATE USES	58
1.4.2 PROHIBITED CERTIFICATE USES	58
1.5 POLICY ADMINISTRATION	59
1.5.1 ORGANIZATION ADMINISTERING THE DOCUMENT	59
1.5.2 CONTACT PERSON	59
1.5.3 PERSON DETERMINING CPS SUITABILITY FOR THE POLICY	60
1.5.4 CPS APPROVAL PROCEDURES	60
1.6 DEFINITIONS AND ACRONYMS	60
1.6.1 DEFINITIONS	60
1.6.2 ACRONYMS	65

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES	68
2.1 REPOSITORIES	68
2.2 PUBLICATION OF CERTIFICATION INFORMATION	68
2.2.1 CERTIFICATION PRACTICES AND CERTIFICATE POLICIES	68
2.2.2 TERMS AND CONDITIONS	68
2.2.3 DISTRIBUTION OF THE CERTIFICATES	68
2.2.4 CRL AND OCSP	69
2.3 TIME OR FREQUENCY OF PUBLICATION	70
2.4 ACCESS CONTROLS TO REPOSITORIES	70
3 IDENTIFICATION AND AUTHENTICATION	71
3.1 NAMING	71
3.1.1 TYPES OF NAMES	71
3.1.2 NEED FOR NAMES TO BE MEANINGFUL	72
3.1.3 PSEUDONYMS	72
3.1.4 RULES USED TO INTERPRET SEVERAL NAME FORMATS	72
3.1.5 UNIQUENESS OF NAMES	72
3.1.6 RECOGNITION, AUTHENTICATION, AND FUNCTION OF REGISTERED TRADEMARKS AND OTHER DISTINCTIVE SYMBOLS	72
3.1.7 NAME DISPUTE RESOLUTION PROCEDURE	73
3.2 INITIAL IDENTITY VALIDATION	73
3.2.1 METHOD TO PROVE POSSESSION OF THE PRIVATE KEY	73
3.2.2 AUTHENTICATION OF ORGANIZATION IDENTITY	74
3.2.2.1 Identity	74
3.2.2.2 Trademarks	74
3.2.2.3 Country verification	74
3.2.2.4 Validation of domain authorization or control	75
3.2.2.5 Authentication of an IP address	75
3.2.2.6 Wildcard Domain Validation	75
3.2.2.7 Accuracy of data sources	75
3.2.2.8 Registros CAA	75
3.2.3 AUTHENTICATION OF INDIVIDUAL IDENTITY	75
3.2.4 NON-VERIFIED SUBSCRIBER INFORMATION	78
3.2.5 VALIDATION OF AUTHORITY	78
3.2.5.1 Verification of association of the Applicant and the Person Responsible with the Entity	78
3.2.5.2 Service or Machine Identity	81
3.2.5.3 Special considerations for issuing certificates outside of Spanish territory	81

3.2.6 CRITERIA FOR INTEROPERATION	81
3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS	81
3.3.1 IDENTIFICATION AND AUTHENTICATION FOR ROUTINE RE-KEY	81
3.3.2 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY AFTER REVOCATION	82
3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST	82
4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS	83
4.1 CERTIFICATE APPLICATION	83
4.1.1 WHO CAN SUBMIT A CERTIFICATE APPLICATION	83
4.1.2 ENROLLMENT PROCESS AND RESPONSIBILITIES	83
4.1.2.1 Web forms	83
4.1.2.2 Batches	84
4.1.2.3 Applications for external TSU and Subordinate CA certificates	84
4.1.2.4 Applications via Web Services (WS) layer	84
4.1.2.5 Cross certification request	85
4.2 CERTIFICATE APPLICATION PROCESSING	85
4.2.1 PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS	85
4.2.2 APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS	85
4.2.3 TIME TO PROCESS CERTIFICATE APPLICATIONS	86
4.3 CERTIFICATE ISSUANCE	86
4.3.1 CA ACTIONS DURING CERTIFICATE ISSUANCE	86
4.3.1.1 Certificates on Software	86
4.3.1.2 Certificates on QSCD SmartCard/Token or on SmartCard/Token	88
4.3.1.3 Certificates issued through Web Services requests	89
4.3.1.4 Certificates on QSCD Cloud or on Cloud	89
4.3.2 NOTIFICATION TO SUBSCRIBER BY THE CA OF ISSUANCE OF CERTIFICATE	89
4.4 CERTIFICATE ACCEPTANCE	89
4.4.1 CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE	89
4.4.2 PUBLICATION OF THE CERTIFICATE BY THE CA	90
4.4.3 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES	90
4.5 KEY PAIR AND CERTIFICATE USAGE	90
4.5.1 SUBSCRIBER PRIVATE KEY AND CERTIFICATE USAGE	90
4.5.2 RELYING PARTY PUBLIC KEY AND CERTIFICATE USAGE	95
4.6 CERTIFICATE RENEWAL	95
4.6.1 CIRCUMSTANCE FOR CERTIFICATE RENEWAL	96
4.6.2 WHO MAY REQUEST RENEWAL	96

4.6.3 PROCESSING CERTIFICATE RENEWAL REQUESTS	96
4.6.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER	96
4.6.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RENEWAL CERTIFICATE	96
4.6.6 PUBLICATION OF THE RENEWAL CERTIFICATE BY THE CA	96
4.6.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES	96
4.7 CERTIFICATE RE-KEY	96
4.7.1 CIRCUMSTANCE FOR CERTIFICATE RE-KEY	96
4.7.2 WHO MAY REQUEST CERTIFICATION OF A NEW PUBLIC KEY	97
4.7.3 PROCESSING CERTIFICATE RE-KEYING REQUESTS	97
4.7.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER	99
4.7.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RE-KEYED CERTIFICATE	99
4.7.6 PUBLICATION OF THE RE-KEYED CERTIFICATE BY THE CA	99
4.7.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES	99
4.8 CERTIFICATE MODIFICATION	99
4.8.1 CIRCUMSTANCE FOR CERTIFICATE MODIFICATION	99
4.8.2 WHO MAY REQUEST CERTIFICATE MODIFICATION	99
4.8.3 PROCESSING CERTIFICATE MODIFICATION REQUESTS	100
4.8.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER	100
4.8.5 CONDUCT CONSTITUTING ACCEPTANCE OF MODIFIED CERTIFICATE	100
4.8.6 PUBLICATION OF THE MODIFIED CERTIFICATE BY THE CA	100
4.8.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES	100
4.9 CERTIFICATE REVOCATION AND SUSPENSION	100
4.9.1 CIRCUMSTANCES FOR REVOCATION	100
4.9.2 WHO CAN REQUEST REVOCATION	103
4.9.3 PROCEDURE FOR REVOCATION REQUEST	103
4.9.4 REVOCATION REQUEST GRACE PERIOD	108
4.9.5 TIME WITHIN WHICH CA MUST PROCESS THE REVOCATION REQUEST	109
4.9.6 REVOCATION CHECKING REQUIREMENT FOR RELYING PARTIES	109
4.9.7 CRL ISSUANCE FREQUENCY	110
4.9.8 MAXIMUM LATENCY FOR CRLS	111
4.9.9 ON-LINE REVOCATION/STATUS CHECKING AVAILABILITY	111
4.9.10 ON-LINE REVOCATION CHECKING REQUIREMENTS	111
4.9.11 OTHER FORMS OF REVOCATION ADVERTISEMENTS AVAILABLE	113
4.9.12 SPECIAL REQUIREMENTS REGARDING PRIVATE KEY COMPROMISE	113
4.9.13 CIRCUMSTANCES FOR SUSPENSION	113
4.9.14 WHO CAN REQUEST SUSPENSION	113

4.9.15 PROCEDURE FOR SUSPENSION REQUEST	114
4.9.16 LIMITS ON SUSPENSION PERIOD	114
4.10 CERTIFICATE STATUS SERVICES	114
4.10.1 OPERATIONAL CHARACTERISTICS	114
4.10.2 SERVICE AVAILABILITY	115
4.10.3 OPTIONAL FEATURES	115
4.11 END OF SUBSCRIPTION	115
4.12 KEY ESCROW AND RECOVERY	116
4.12.1 KEY ESCROW AND RECOVERY POLICY AND PRACTICES	116
4.12.2 SESSION KEY ENCAPSULATION AND RECOVERY POLICY AND PRACTICES	116
5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS	117
5.1 PHYSICAL CONTROLS	117
5.1.1 SITE LOCATION AND CONSTRUCTION	117
5.1.2 PHYSICAL ACCESS	118
5.1.3 POWER AND AIR CONDITIONING	118
5.1.4 WATER EXPOSURE	118
5.1.5 FIRE PREVENTION AND PROTECTION	118
5.1.6 MEDIA STORAGE	118
5.1.7 WASTE DISPOSAL	119
5.1.8 OFF-SITE BACKUP	119
5.2 PROCEDURAL CONTROLS	119
5.2.1 TRUSTED ROLES	119
5.2.2 NUMBER OF PERSONS REQUIRED PER TASK	120
5.2.3 IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE	120
5.2.4 ROLES REQUIRING SEPARATION OF DUTIES	120
5.3 PERSONNEL CONTROLS	120
5.3.1 QUALIFICATIONS, EXPERIENCE, AND CLEARANCE REQUIREMENTS	120
5.3.2 BACKGROUND CHECK PROCEDURES	121
5.3.3 TRAINING REQUIREMENTS	121
5.3.4 RETRAINING FREQUENCY AND REQUIREMENTS	122
5.3.5 JOB ROTATION FREQUENCY AND SEQUENCE	122
5.3.6 SANCTIONS FOR UNAUTHORIZED ACTIONS	122
5.3.7 INDEPENDENT CONTRACTOR REQUIREMENTS	122
5.3.8 DOCUMENTATION SUPPLIED TO PERSONNEL	122
5.4 AUDIT LOGGING PROCEDURES	123

5.4.1 TYPES OF EVENTS RECORDED	123
5.4.2 FREQUENCY OF PROCESSING LOG	124
5.4.3 RETENTION PERIOD FOR AUDIT LOGS	124
5.4.4 PROTECTION OF AUDIT LOG	124
5.4.5 AUDIT LOG BACKUP PROCEDURES	125
5.4.6 AUDIT COLLECTION SYSTEM (INTERNAL VS. EXTERNAL)	125
5.4.7 NOTIFICATION TO EVENT-CAUSING SUBJECT	125
5.4.8 VULNERABILITY ASSESSMENTS	125
5.5 RECORDS ARCHIVAL	126
5.5.1 TYPES OF RECORDS ARCHIVED	126
5.5.2 RETENTION PERIOD FOR ARCHIVE	126
5.5.3 PROTECTION OF ARCHIVE	126
5.5.4 ARCHIVE BACKUP PROCEDURES	126
5.5.5 REQUIREMENTS FOR TIME-STAMPING OF RECORDS	127
5.5.6 ARCHIVE COLLECTION SYSTEM (INTERNAL OR EXTERNAL)	127
5.5.7 PROCEDURES TO OBTAIN AND VERIFY ARCHIVE INFORMATION	127
5.6 KEY CHANGEOVER	127
5.7 COMPROMISE AND DISASTER RECOVERY	128
5.7.1 INCIDENT AND COMPROMISE HANDLING PROCEDURES	128
5.7.2 COMPUTING RESOURCES, SOFTWARE, AND/OR DATA ARE CORRUPTED	128
5.7.3 ENTITY PRIVATE KEY COMPROMISE PROCEDURES	128
5.7.4 BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER	130
5.8 CA OR RA TERMINATION	130
5.8.1 CESSATION OF ACTIVITY	130
5.8.2 TERMINATION OF A CA	131
5.8.3 TERMINATION OF A RA	133
6 TECHNICAL SECURITY CONTROLS	134
6.1 KEY PAIR GENERATION AND INSTALLATION	134
6.1.1 KEY PAIR GENERATION	134
6.1.1.1 Creating the Subject's key pair	135
6.1.1.2 Key creation hardware/software	136
6.1.2 PRIVATE KEY DELIVERY TO SUBSCRIBER	136
6.1.3 PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER	136
6.1.4 CA PUBLIC KEY DELIVERY TO RELYING PARTIES	136
6.1.5 KEY SIZES	136

6.1.6 PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING	136
6.1.7 KEY USAGE PURPOSES (AS PER X.509 V3 KEY USAGE FIELD)	137
6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS	137
6.2.1 CRYPTOGRAPHIC MODULE STANDARDS AND CONTROLS	137
6.2.1.1 The CA's private key	137
6.2.1.2 The Subject's private key	138
6.2.2 PRIVATE KEY (N OUT OF M) MULTI-PERSON CONTROL	139
6.2.3 PRIVATE KEY ESCROW	139
6.2.4 PRIVATE KEY BACKUP	139
6.2.5 PRIVATE KEY ARCHIVAL	139
6.2.6 PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE	140
6.2.7 PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE	140
6.2.8 METHOD OF ACTIVATING PRIVATE KEY	140
6.2.9 METHOD OF DEACTIVATING PRIVATE KEY	141
6.2.10 METHOD OF DESTROYING PRIVATE KEY	141
6.2.11 CRYPTOGRAPHIC MODULE RATING	141
6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT	141
6.3.1 PUBLIC KEY ARCHIVAL	141
6.3.2 CERTIFICATE OPERATIONAL PERIODS AND KEY PAIR USAGE PERIODS	142
6.4 ACTIVATION DATA	142
6.4.1 ACTIVATION DATA GENERATION AND INSTALLATION	142
6.4.2 ACTIVATION DATA PROTECTION	143
6.4.3 OTHER ASPECTS OF ACTIVATION DATA	143
6.5 COMPUTER SECURITY CONTROLS	143
6.5.1 SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS	144
6.5.2 COMPUTER SECURITY RATING	144
6.6 LIFE CYCLE TECHNICAL CONTROLS	144
6.6.1 SYSTEM DEVELOPMENT CONTROLS	145
6.6.2 SECURITY MANAGEMENT CONTROLS	145
6.6.2.1 Security Management	145
6.6.2.2 Data and asset classification and management	145
6.6.2.3 Management procedures	145
6.6.2.4 Tratamiento de los soportes y seguridad	146
6.6.2.5 System planning	146
6.6.2.6 Incident reporting and response	146
6.6.2.7 Operating procedures and responsibilities	146

6.6.2.8 Access system management	146
6.6.2.9 Managing the cryptographic hardware lifecycle	147
6.6.3 LIFE CYCLE SECURITY CONTROLS	147
6.7 NETWORK SECURITY CONTROLS	148
6.8 TIME-STAMPING	148
7 CERTIFICATE, CRL, AND OCSP PROFILES	149
7.1 CERTIFICATE PROFILE	149
7.1.1 VERSION NUMBER	149
7.1.2 CERTIFICATE EXTENSIONS	149
7.1.3 ALGORITHM OBJECT IDENTIFIERS	149
7.1.4 NAME FORMS	149
7.1.5 NAME CONSTRAINTS	150
7.1.6 CERTIFICATE POLICY OBJECT IDENTIFIER	150
7.1.7 USAGE OF POLICY CONSTRAINTS EXTENSION	150
7.1.8 POLICY QUALIFIERS SYNTAX AND SEMANTICS	151
7.1.9 PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICIES EXTENSION	151
7.2 CRL PROFILE	151
7.2.1 VERSION NUMBER	151
7.2.2 CRL AND CRL ENTRY EXTENSIONS	151
7.3 OCSP PROFILE	151
7.3.1 VERSION NUMBER	152
7.3.2 OCSP EXTENSIONS	152
8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS	153
8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT	153
8.1.1 EXTERNAL SUBORDINATE CA AUDITS OR CROSS-CERTIFICATION	154
8.1.2 AUDITING THE RAS	154
8.1.3 SELF-AUDITS	154
8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR	154
8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY	154
8.4 TOPICS COVERED BY ASSESSMENT	155
8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY	155
8.6 COMMUNICATION OF RESULTS	155
9 OTHER BUSINESS AND LEGAL MATTERS	156
9.1 FEES	156
9.1.1 CERTIFICATE ISSUANCE OR RENEWAL FEES	156

9.1.2 CERTIFICATE ACCESS FEES	156
9.1.3 REVOCATION OR STATUS INFORMATION ACCESS FEES	156
9.1.4 FEES FOR OTHER SERVICES	156
9.1.5 REFUND POLICY	156
9.2 FINANCIAL RESPONSIBILITY	157
9.2.1 INSURANCE COVERAGE	157
9.2.2 OTHER ASSETS	157
9.2.3 INSURANCE OR WARRANTY COVERAGE FOR END-ENTITIES	157
9.3 CONFIDENTIALITY OF BUSINESS INFORMATION	157
9.3.1 SCOPE OF BUSINESS INFORMATION	157
9.3.2 INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION	157
9.3.3 RESPONSIBILITY TO PROTECT CONFIDENTIAL INFORMATION	158
9.3.3.1 Disclosure of information about certificate revocation/suspension	158
9.3.3.2 Sending information to the Competent Authority	158
9.4 PRIVACY OF PERSONAL INFORMATION	158
9.4.1 PRIVACY PLAN	158
9.4.2 INFORMATION TREATED AS PRIVATE	158
9.4.3 INFORMATION NOT DEEMED PRIVATE	159
9.4.4 RESPONSIBILITY TO PROTECT PRIVATE INFORMATION	159
9.4.5 NOTICE AND CONSENT TO USE PRIVATE INFORMATION	159
9.4.6 DISCLOSURE PURSUANT TO JUDICIAL OR ADMINISTRATIVE PROCESS	159
9.4.7 OTHER INFORMATION DISCLOSURE CIRCUMSTANCES	159
9.5 INTELLECTUAL PROPERTY RIGHTS	159
9.6 REPRESENTATIONS AND WARRANTIES	159
9.6.1 CA REPRESENTATIONS AND WARRANTIES	159
9.6.1.1 CAs under this CPS	160
9.6.1.2 External Subordinate CAs	162
9.6.2 RA REPRESENTATIONS AND WARRANTIES	162
9.6.3 SUBSCRIBER REPRESENTATIONS AND WARRANTIES	165
9.6.3.1 Subscriber	165
9.6.3.2 Applicant	165
9.6.3.3 Subject and Person Responsible	166
9.6.3.4 Entity	168
9.6.4 RELYING PARTY REPRESENTATIONS AND WARRANTIES	168
9.6.5 REPRESENTATIONS AND WARRANTIES OF OTHER PARTICIPANTS	169
9.7 DISCLAIMERS OF WARRANTIES	169

9.8 LIMITATIONS OF LIABILITY	170
9.9 INDEMNITIES	170
9.10 TERM AND TERMINATION	170
9.10.1 TERM	170
9.10.2 TERMINATION	170
9.10.3 EFFECT OF TERMINATION AND SURVIVAL	170
9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS	170
9.12 AMENDMENTS	170
9.12.1 PROCEDURE FOR AMENDMENT	171
9.12.2 NOTIFICATION MECHANISM AND PERIOD	171
9.12.2.1 List of aspects	171
9.12.2.2 Notification method	171
9.12.2.3 Period for comments	171
9.12.2.4 Comment processing system	171
9.12.3 CIRCUMSTANCES UNDER WHICH OID MUST BE CHANGED	172
9.13 DISPUTE RESOLUTION PROCEDURE	172
9.14 GOVERNING LAW	172
9.15 COMPLIANCE WITH APPLICABLE LAW	172
9.16 MISCELLANEOUS PROVISIONS	172
9.16.1 ENTIRE AGREEMENT	172
9.16.2 ASSIGNMENT	172
9.16.3 SEVERABILITY	172
9.16.4 ENFORCEMENT (ATTORNEYS' FEES AND WAIVER OF RIGHTS)	173
9.16.5 FORCE MAJEURE	173
9.17 OTHER PROVISIONS	173
APPENDICE 1 DOCUMENT HISTORY	174

1 INTRODUCTION

1.1 OVERVIEW

In this document and in accordance with IETF RFC 3647 standard:

- Certificate Policy (hereinafter, CP): a set of rules defining the applicability of a end entity certificate to a community and/or a set of applications or uses with common security requirements.
- Certification Practice Statement (hereinafter, CPS): a set of practices adopted by a Certification Authority (hereinafter, CA) for the issuance, management, revocation, and renewal or re-key of certificates. It contains detailed information about its certificate security, support, administration, issuing (including renewing or re-keying) and revoking systems, as well as the trust relationship among the CA, the Subject and the Relying Party. It accurately describes the services provided, detailed certificate lifecycle management procedures, etc.

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

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

Regulation (EU) No 910/2014 of the European Parliament and of the Council, of 23 July 2014, on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (hereinafter, referred to as eIDAS Regulation) defines a ‘trust service’ as an electronic service normally provided for remuneration which consist of:

- a) the creation, verification and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or
- b) the creation, verification and validation of certificates for website authentication, or
- c) the preservation of electronic signatures, seals or certificates related to those services.

The ETSI EN 319 401 standard defines a ‘trust service’ as an electronic service for:

- creation, verification and validation of digital signatures and related certificates;
- creation, verification and validation of time-stamps and related certificates;
- registered delivery and related certificates;
- creation, verification and validation of certificates for website authentication; or
- preservation of digital signatures or certificates related to those services.

This document specifies the CPS and the CPs for the issuance of certificates by AC Camerfirma SA (hereinafter, Camerfirma) active CAs under 2008, 2016, 2021 and 2024 Camerfirma hierarchies (Chambers of Commerce Root – 2008, CHAMBERS OF COMMERCE ROOT – 2016, GLOBAL CHAMBERSIGN ROOT – 2016, CAMERFIRMA ROOT 2021) and (INFOCERT-CAMERFIRMA ROOT 2024), in accordance with eIDAS Regulation and based on the following ETSI standards:

Service	ETSI general	ETSI scope	ETSI profiles
Issuance of end entity certificates to natural persons (including certificates for electronic signatures and qualified certificates for electronic signatures, in accordance with eIDAS Regulation)	EN 319 401 v2.3.1: General Policy Requirements for Trust Service Providers	EN 319 411-1 v1.3.1: Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements EN 319 411-2 v2.4.1: Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates	EN 319 412-1 v1.5.1: Certificate Profiles; Part 1: Overview and common data structures EN 319 412-2 v2.3.1: Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons EN 319 412-5 v2.4.1: Certificate Profiles ; Part 5 : QcStatements
Issuance of end entity certificates to legal persons (certificates for electronic seals and qualified certificates for electronic seals, in accordance with eIDAS Regulation; including OCSP certificates; excluding certificates for digital signing of time-stamps)	EN 319 401 v2.3.1: General Policy Requirements for Trust Service Providers	EN 319 411-1 v1.3.1: Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements EN 319 411-2 v2.4.1: Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates	EN 319 412-1 v1.5.1: Certificate Profiles; Part 1: Overview and common data structures EN 319 412-2 v2.3.1: Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons EN 319 412-3 v1.3.1: Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons EN 319 412-5 v2.4.1:

			Certificate Profiles ; Part 5 : QcStatements
Issuance of end entity certificates to legal persons for digital signing of time-stamps (including electronic time stamps and qualified electronic time stamps, in accordance with eIDAS Regulation)	EN 319 401 v2.3.1: General Policy Requirements for Trust Service Providers	EN 319 411-1 v1.3.1: Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements EN 319 411-2 v2.4.1: Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates EN 319 421 v1.2.1: Policy and Security Requirements for Trust Service Providers issuing Time-Stamps	EN 319 412-1 v1.5.1: Certificate Profiles; Part 1: Overview and common data structures EN 319 412-2 v2.3.1: Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons EN 319 412-3 v1.3.1: Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons EN 319 422 v1.1.1: Time-stamping protocol and time-stamp token profiles
Issuance of CA certificates to legal persons (certificates for electronic seals, in accordance with eIDAS Regulation; including certificates for Camerfirma CAs and certificates for CAs of other legal persons)	EN 319 401 v2.3.1: General Policy Requirements for Trust Service Providers	EN 319 411-1 v1.4.1: Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements	

In addition, the CPS and the CPs in this document are compliant with the Spanish Law 6/2020, of 11 November, regulating certain aspects of electronic trust services (hereinafter, Law 6/2020).

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

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

- NCP Normalized Certificate Policy. Meets general recognized best practice for trust service providers issuing certificates used in support of any type of transaction.
- NCP+ Extended Normalized Certificate Policy. NCP requiring a secure cryptographic device. Includes all the NCP policy requirements, plus additional requirements suited to support the use of a secure cryptographic device (for signing and/or decrypting).
- 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. If the implementation requires a secure cryptographic device, 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 28 of the eIDAS Regulation.
- QCP-n-qscd Certificate Policy for EU Qualified Certificates issued to natural persons with private key related to the certified public key in a Qualified Electronic Signature Creation Device (hereinafter, QSCD). Includes all the QCP-n policy requirements (including all the NCP+ policy requirements), plus additional requirements 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-I 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. If the implementation requires a secure cryptographic device, 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 seals based on a qualified certificate defined in articles 36 and 38 of the eIDAS Regulation.
- QCP-I-qscd Certificate Policy for EU Qualified Certificates issued to legal persons with private key related to the certified public key in a Qualified Electronic Seal Creation Device (hereinafter, QSCD). Includes all the QCP-I policy requirements (including all the NCP+ policy requirements), plus additional

requirements 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 seals such as defined in article 3 (27) of the eIDAS Regulation.

CAs under the CPS in this document (hereinafter, this CPS) issue qualified certificates on QSCD devices and on Non-QSCD devices and non-qualified certificates on Non-QSCD devices –in the case of end entity certificates, under the CPs in this document (hereinafter, these CPs)–, with keys generated in:

- QSCD SmartCard/Token:
 - QSCD cryptographic smartcards.
 - QSCD cryptographic tokens.
- QSCD Cloud:
 - QSCD centralized platform managed by Camerfirma or another QTSP.
- QSCD HSM:
 - QSCD HSM managed by Camerfirma or another TSP. Only for TSU certificates.
- Non-QSCD:
 - P12:
 - Software (PKCS #12).
 - CSR:
 - Non-QSCD or QSCD external device not managed by Camerfirma. Through a certificate signing request in PKCS #10 format
 - SmartCard/Token (secure cryptographic device):
 - Non-QSCD or QSCD cryptographic smartcards.
 - Non-QSCD or QSCD cryptographic tokens.
 - Cloud (secure cryptographic device):
 - Non-QSCD or QSCD centralized platform managed by Camerfirma or another TSP.
 - HSM (secure cryptographic device):
 - Non-QSCD or QSCD HSM managed by Camerfirma or another TSP. Only for TSU, CA and OCSP certificates.

This document is structured in accordance with IETF RFC 3647 standard.

1.2 DOCUMENT NAME AND IDENTIFICATION

Name:	Certification Practice Statement and Certificate Policies CAMERFIRMA
Description:	Certification Practice Statement and Certificate Policies for Camerfirma active CAs under 2008 ,2016, 2021 and 2024 Camerfirma hierarchies (Chambers of Commerce Root – 2008, CHAMBERS OF COMMERCE ROOT – 2016, GLOBAL CHAMBERSIGN ROOT – 2016, CAMERFIRMA ROOT 2021) and 2024 (INFOCERT-CAMERFIRMA ROOT 2024)
Version:	See homepage
OIDs:	<ul style="list-style-type: none"> • 1.3.6.1.4.1.17326.10.1: CPS • CPs Qualified Citizen Certificate CHAMBERS OF COMMERCE ROOT – 2016 hierarchy <ul style="list-style-type: none"> ○ 1.3.6.1.4.1.17326.10.16.1.1.1: QSCD SmartCard/Token ○ 1.3.6.1.4.1.17326.10.16.1.1.1, 1.3.6.1.4.1.17326.99.18.1: QSCD Cloud ○ 1.3.6.1.4.1.17326.10.16.1.1.2: Non-QSCD CHAMERFIRMA ROOT 2021 hierarchy <ul style="list-style-type: none"> ○ 1.3.6.1.4.1.17326.10.21.1.1.1: QSCD SmartCard/Token ○ 1.3.6.1.4.1.17326.10.21.1.1.3: QSCD Cloud INFOCERT-CAMERFIRMA ROOT 2024 hierarchy <ul style="list-style-type: none"> ○ 1.3.6.1.4.1.17326.10.21.1.1.2: Non-QSCD • CPs Qualified Corporate Certificate / Qualified Certificate for a Self-employed / Qualified Certificate for a Chartered Self-employed CHAMBERS OF COMMERCE ROOT – 2016 hierarchy <ul style="list-style-type: none"> ○ 1.3.6.1.4.1.17326.10.16.1.2.1: QSCD SmartCard/Token ○ 1.3.6.1.4.1.17326.10.16.1.2.1, 1.3.6.1.4.1.17326.99.18.1: QSCD Cloud ○ 1.3.6.1.4.1.17326.10.16.1.2.2 - Non-QSCD CHAMERFIRMA ROOT 2021 hierarchy <ul style="list-style-type: none"> ○ 1.3.6.1.4.1.17326.10.21.1.2.1: QSCD SmartCard/Token ○ 1.3.6.1.4.1.17326.10.21.1.2.3: QSCD Cloud • CPs Qualified Certificates for a Representative CHAMBERS OF COMMERCE ROOT – 2016 hierarchy <ul style="list-style-type: none"> ○ Legal Representative of a Legal/Non-Legal Entity <ul style="list-style-type: none"> ▪ 1.3.6.1.4.1.17326.10.16.1.3.1.1: QSCD SmartCard/Token ▪ 1.3.6.1.4.1.17326.10.16.1.3.1.1, 1.3.6.1.4.1.17326.99.18.1: QSCD Cloud ▪ 1.3.6.1.4.1.17326.10.16.1.3.1.2: Non-QSCD ○ Voluntary Representative of a Legal/Non-Legal Entity before the Public Administrations <ul style="list-style-type: none"> ▪ 1.3.6.1.4.1.17326.10.16.1.3.2.1: QSCD SmartCard/Token ▪ 1.3.6.1.4.1.17326.10.16.1.3.2.1, 1.3.6.1.4.1.17326.99.18.1: QSCD Cloud ▪ 1.3.6.1.4.1.17326.10.16.1.3.2.2: Non-QSCD ○ Special Representative of a Legal/Non-Legal Entity <ul style="list-style-type: none"> ▪ 1.3.6.1.4.1.17326.10.16.1.3.3.1: QSCD SmartCard/Token ▪ 1.3.6.1.4.1.17326.10.16.1.3.3.1, 1.3.6.1.4.1.17326.99.18.1: QSCD Cloud ▪ 1.3.6.1.4.1.17326.10.16.1.3.3.2: Non-QSCD CHAMERFIRMA ROOT 2021 hierarchy

- Legal Representative of a Legal Entity
 - 1.3.6.1.4.1.17326.10.21.1.3.1: QSCD SmartCard/Token
 - 1.3.6.1.4.1.17326.10.21.1.3.3: QSCD Cloud
- Legal Representative of a Non-Legal Entity
 - 1.3.6.1.4.1.17326.10.21.1.4.1: QSCD SmartCard/Token
 - 1.3.6.1.4.1.17326.10.21.1.4.3: QSCD Cloud
- Voluntary Representative of a Legal Entity before the Public Administrations
 - 1.3.6.1.4.1.17326.10.21.1.5.1: QSCD SmartCard/Token
 - 1.3.6.1.4.1.17326.10.21.1.5.3: QSCD Cloud
- Voluntary Representative of a Non-Legal Entity before the Public Administrations
 - 1.3.6.1.4.1.17326.10.21.1.6.1: QSCD SmartCard/Token
 - 1.3.6.1.4.1.17326.10.21.1.6.3: QSCD Cloud
- Special Representative of a Legal Entity
 - 1.3.6.1.4.1.17326.10.21.1.7.1: QSCD SmartCard/Token
 - 1.3.6.1.4.1.17326.10.21.1.7.3: QSCD Cloud
- Special Representative of a Non-Legal Entity
 - 1.3.6.1.4.1.17326.10.21.1.8.1: QSCD SmartCard/Token
 - 1.3.6.1.4.1.17326.10.21.1.8.3: QSCD Cloud
- **CPs Certificates for a Public Employee With/Without a Pseudonym**
CHAMBERS OF COMMERCE ROOT – 2016 hierarchy
 - Qualified Certificate for Signature - High Level
 - 1.3.6.1.4.1.17326.10.16.1.5.1.3.4.1: QSCD SmartCard/Token
 - 1.3.6.1.4.1.17326.10.16.1.5.1.3.4.1, 1.3.6.1.4.1.17326.99.18.1: QSCD Cloud
 - Non-Qualified Certificate for Authentication - High Level
 - 1.3.6.1.4.1.17326.10.16.1.5.1.3.4.2: SmartCard/Token
 - 1.3.6.1.4.1.17326.10.16.1.5.1.3.4.2, 1.3.6.1.4.1.17326.99.18.1: Cloud
 - Non-Qualified Certificate for Encipherment - High Level
 - 1.3.6.1.4.1.17326.10.16.1.5.1.3.4.3: SmartCard/Token
 - 1.3.6.1.4.1.17326.10.16.1.5.1.3.4.3, 1.3.6.1.4.1.17326.99.18.1: Cloud
 - Qualified Certificate - Medium Level
 - 1.3.6.1.4.1.17326.10.16.1.5.1.3.4.4: QSCD SmartCard/Token / Non-QSCD
 - 1.3.6.1.4.1.17326.10.16.1.5.1.3.4.4, 1.3.6.1.4.1.17326.99.18.1: QSCD Cloud
- **CPs Qualified Certificate for Electronic Seal**
CHAMBERS OF COMMERCE ROOT – 2016 hierarchy
 - 1.3.6.1.4.1.17326.10.16.2.1.1: QSCD SmartCard/Token
 - 1.3.6.1.4.1.17326.10.16.2.1.2: Non-QSCD
- **CPs Qualified Certificate for Electronic Seal for Public Administrations**
CHAMBERS OF COMMERCE ROOT – 2016 hierarchy
 - 1.3.6.1.4.1.17326.10.16.2.2.1.3.3.1: High Level - QSCD SmartCard/Token
 - 1.3.6.1.4.1.17326.10.16.2.2.1.4.3.1: Medium Level - Non-QSCD
- **CP TSU Qualified Certificate**
CHAMBERS OF COMMERCE ROOT – 2016 hierarchy
 - 1.3.6.1.4.1.17326.10.16.5.1.1 - QSCD HSM (no new certificates are issued)
 INFOCERT-CAMERFIRMA ROOT 2024 hierarchy

- 1.3.6.1.4.1.17326.10.21.30.4 - QSCD HSM
- **CPs TSU Non-Qualified Certificate**
Chambers of Commerce Root – 2008 hierarchy
 - 1.3.6.1.4.1.17326.10.13.1.3: HSM
- **CP Code Signing Non-Qualified Certificate**
Chambers of Commerce Root – 2008 hierarchy
 - 1.3.6.1.4.1.17326.10.12.2
- **CPs Non-Qualified Certificate for Electronic Seal**
Chambers of Commerce Root – 2008 hierarchy
 - 1.3.6.1.4.1.17326.10.11.3.1.1: P12
 - 1.3.6.1.4.1.17326.10.11.3.1.2: CSR
- **CP Non-Qualified Certificate for Electronic Seal for Public Administrations**
Chambers of Commerce Root – 2008 hierarchy
 - 1.3.6.1.4.1.17326.1.3.3.2 (no new certificates are issued)
- **CP Non-Qualified Certificate for Personnel for Public Administrations**
Chambers of Commerce Root – 2008 hierarchy
 - 1.3.6.1.4.1.17326.1.3.4.4 (no new certificates are issued)
- **CPs Non-Qualified OCSP Certificate**
Chambers of Commerce Root – 2008, CHAMBERS OF COMMERCE ROOT – 2016, GLOBAL CHAMBERSIGN ROOT – 2016 hierarchies
 - 1.3.6.1.4.1.17326.10.9.8: HSM
 CAMERFIRMA ROOT 2021 hierarchy
 - 1.3.6.1.4.1.17326.10.21.0.1: HSM

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

1.3 PKI PARTICIPANTS

1.3.1 CERTIFICATION AUTHORITIES (CAS)

A CA is a component of a PKI responsible for issuing and managing certificates. A CA is a type of Trust Service Provider (TSP) that issues certificates. It acts as the trusted third party between the Subject and the Relying Party, 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 attribute *organization* (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 de Rodríguez Marín 88 – 28016 Madrid

Telephone: +34 91 136 91 05
Email: ca@camerfirma.com / info@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/s) for checking and storing the documentation regarding the content of end entity certificates. Under this 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 Subordinate CAs (also known as Intermediate CAs).

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

A Subordinate CA obtains a certificate from the Root CA to issue end entity certificates and/or other Subordinate CA certificates. The number of Subordinate CAs allowed under a Root or Subordinate CA has been specified in the *Basic Constraints* extension (*pathLenConstraint* field) of the CA certificate.

The following sections describe the CAs hierarchies that Camerfirma manages as the owner under this CPS. In the case of Subordinate CA owned by another organization (hereinafter, external Subordinate CA/s), this CPS will refer to its existence within the corresponding hierarchy due to its subjection to the Root CA or to a Subordinate CA owned by Camerfirma, but it will be governed by its own CPS and 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
- CAMERFIRMA ROOT 2021
- INFOCERT-CAMERFIRMA ROOT 2024

1.3.1.1 CHAMBERS OF COMMERCE ROOT HIERARCHIES

CHAMBERS OF COMMERCE ROOT IN ITS DIFFERENT VERSIONS IS PROPERTY OF AC CAMERFIRMA SA AS INDICATED IN THE ATTRIBUTE *ORGANIZATION* OF THE FIELD *SUBJECT* OF THE CORRESPONDING ROOT CAS CERTIFICATES.

These hierarchies are designed to develop a trusted network with the aim of issuing certificates to natural persons, with or without attributes of association with public or private entities, and to public or private entities within the European Union, and in which the CAs are established in Spain, and the RAs are managed by the Spanish Chambers of Commerce, Industry and Navigation or by public or private entities with no territorial limitations. EXCEPTION: TSU certificates have no territorial limitations.

Under these hierarchies, certificates can be issued by Subordinate CAs established in Spain corresponding to a specific business, institution or public group can be issued, provided that the territorial scope of certificates is the European Union, and CAs and RAs meet the requirements set by Camerfirma, always subject to the applicable laws and regulations in force.

The Subordinate CAs that issue certificates under these hierarchies may be owned by Camerfirma or by other TSPs. All the CAs that operate under these hierarchies do so from infrastructures technically controlled by Camerfirma.

The identification details for the active Root CAs certificates of these hierarchies are:

- **CHAMBERS OF COMMERCE ROOT – 2016**
CN: CHAMBERS OF COMMERCE ROOT - 2016
Valid from (UTC time): 14/04/2016 07:35:48
Valid until (UTC time): 08/04/2040 07:35:48
Serial Number: 349A 2DA1 8206 B2B3
X509v3 Subject Key Identifier: 9E2E 654F 3E57 F5AB 7D96 C68B DFB3 356D 4AE8 9E8B
Hash SHA-1: 2DE1 6A56 77BA CA39 E1D6 8C30 DCB1 4ABE 22A6 179B
Hash SHA-256: 04F1 BEC3 6951 BC14 54A9 04CE 3289 0C5D A3CD E135 6B79 00F6 E62D FA20 41EB AD51
- **Chambers of Commerce Root – 2008** (certificate with SHA-1 signature)
CN: Chambers of Commerce Root - 2008
Valid from (UTC time): 01/08/2008 12:29:50
Valid until (UTC time): 31/07/2038 12:29:50
Serial Number: 00 A3DA 427E A4B1 AEDA
X509v3 Subject Key Identifier: F924 AC0F B2B5 F879 C0FA 6088 1BC4 D94D 029E 1719
Hash SHA-1: 786A 74AC 76AB 147F 9C6A 3050 BA9E A87E FE9A CE3C
Hash SHA-256: 063E 4AFA C491 DFD3 32F3 089B 8542 E946 17D8 93D7 FE94 4E10 A793 7EE2 9D96 93C0
- **Chambers of Commerce Root – 2008** (certificate with same keys and SHA-256 signature)
CN: Chambers of Commerce Root - 2008
Valid from (UTC time): 07/12/2011 11:28:07

Valid until (UTC time): 31/07/2038 11:28:07

Serial Number: 00 D908 3FBB A967 CA1A

X509v3 Subject Key Identifier: F924 AC0F B2B5 F879 C0FA 6088 1BC4 D94D 029E 1719

Hash SHA-1: CD03 B468 3048 E364 B8E9 F7ED D94C 7874 7C39 51CA

Hash SHA-256: 3666 F804 9140 FDC0 A65E 809B 281A 3BE3 B10D AFEE FD76 B9DD C272 A93E 83CA 5B99

The following table shows the scheme of active Root CAs and Subordinate CAs under these hierarchies, including, where applicable, the respective OIDs in the *Certificate Policies* extension of the certificates of each CA and/or of the different types of active end entity certificates issued by each Subordinate CA under this CPS.

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

0.4.0.194112.1.0 [ETSI EN 319 411-2 – QCP-n]	Qualified Certificate for a Self-employed – Non-QSCD Qualified Certificate for a Chartered Self-employed – Non-QSCD
1.3.6.1.4.1.17326.10.16.1.3.1.1 [Camerfirma] 2.16.724.1.3.5.8 [national regulations - representative of a legal person] 0.4.0.194112.1.2 [ETSI EN 319 411-2 – QCP-n-qscd]	Qualified Certificate for a Legal Representative of a Legal Entity – QSCD SmartCard/Token
1.3.6.1.4.1.17326.10.16.1.3.1.1 [Camerfirma] 2.16.724.1.3.5.9 [national regulations - representative of a non-legal entity] 0.4.0.194112.1.2 [ETSI EN 319 411-2 – QCP-n-qscd]	Qualified Certificate for a Legal Representative of a Non-Legal Entity – QSCD SmartCard/Token
1.3.6.1.4.1.17326.10.16.1.3.1.1 [Camerfirma] 1.3.6.1.4.1.17326.99.18.1 [Camerfirma] 2.16.724.1.3.5.8 [national regulations - representative of a legal person] 0.4.0.194112.1.2 [ETSI EN 319 411-2 – QCP-n-qscd]	Qualified Certificate for a Legal Representative of a Legal Entity – QSCD Cloud
1.3.6.1.4.1.17326.10.16.1.3.1.1 [Camerfirma] 1.3.6.1.4.1.17326.99.18.1 [Camerfirma] 2.16.724.1.3.5.9 [national regulations - representative of a non-legal entity] 0.4.0.194112.1.2 [ETSI EN 319 411-2 – QCP-n-qscd]	Qualified Certificate for a Legal Representative of a Non-Legal Entity – QSCD Cloud
1.3.6.1.4.1.17326.10.16.1.3.1.2 [Camerfirma] 2.16.724.1.3.5.8 [national regulations - representative of a legal person] 0.4.0.194112.1.0 [ETSI EN 319 411-2 – QCP-n]	Qualified Certificate for a Legal Representative of a Legal Entity – Non-QSCD
1.3.6.1.4.1.17326.10.16.1.3.1.2 [Camerfirma] 2.16.724.1.3.5.9 [national regulations - representative of a non-legal entity] 0.4.0.194112.1.0 [ETSI EN 319 411-2 – QCP-n]	Qualified Certificate for a Legal Representative of a Non-Legal Entity – Non-QSCD
1.3.6.1.4.1.17326.10.16.1.3.2.1 [Camerfirma] 2.16.724.1.3.5.8 [national regulations - representative of a legal person]	Qualified Certificate for a Voluntary Representative of a Legal Entity before the Public Administrations – QSCD SmartCard/Token

0.4.0.194112.1.2 [ETSI EN 319 411-2 – QCP-n-qscd]	
1.3.6.1.4.1.17326.10.16.1.3.2.1 [Camerfirma] 2.16.724.1.3.5.9 [national regulations - representative of a non-legal entity] 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 – QSCD SmartCard/Token
1.3.6.1.4.1.17326.10.16.1.3.2.1 [Camerfirma] 1.3.6.1.4.1.17326.99.18.1 [Camerfirma] 2.16.724.1.3.5.8 [national regulations - representative of a legal person] 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 – QSCD Cloud
1.3.6.1.4.1.17326.10.16.1.3.2.1 [Camerfirma] 1.3.6.1.4.1.17326.99.18.1 [Camerfirma] 2.16.724.1.3.5.9 [national regulations - representative of a non-legal entity] 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 – QSCD Cloud
1.3.6.1.4.1.17326.10.16.1.3.2.2 [Camerfirma] 2.16.724.1.3.5.8 [national regulations - representative of a legal person] 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 – Non-QSCD
1.3.6.1.4.1.17326.10.16.1.3.2.2 [Camerfirma] 2.16.724.1.3.5.9 [national regulations - representative of a non-legal entity] 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 – Non-QSCD
1.3.6.1.4.1.17326.10.16.1.3.3.1 [Camerfirma] 0.4.0.194112.1.2 [ETSI EN 319 411-2 – QCP-n-qscd]	Qualified Certificate for a Special Representative of a Legal/Non-Legal Entity – QSCD SmartCard/Token
1.3.6.1.4.1.17326.10.16.1.3.3.1 [Camerfirma] 1.3.6.1.4.1.17326.99.18.1 [Camerfirma] 0.4.0.194112.1.2 [ETSI EN 319 411-2 – QCP-n-qscd]	Qualified Certificate for a Special Representative of a Legal/Non-Legal Entity – QSCD Cloud
1.3.6.1.4.1.17326.10.16.1.3.3.2 [Camerfirma] 0.4.0.194112.1.0 [ETSI EN 319 411-2 – QCP-n]	Qualified Certificate for a Special Representative of a Legal/Non-Legal Entity – Non-QSCD
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.1 [Camerfirma] 2.16.724.1.3.5.7.1 [national regulations -	Qualified Certificate for Signature for a Public Employee – High Level –

Public Administrations - public employee - high level] 0.4.0.194112.1.2 [ETSI EN 319 411-2 – QCP-n-qscd]	QSCD SmartCard/Token
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.1 [Camerfirma] 2.16.724.1.3.5.4.1 [national regulations - Public Administrations - public employee under a pseudonym - high level] 0.4.0.194112.1.2 [ETSI EN 319 411-2 – QCP-n-qscd]	Qualified Certificate for Signature for a Public Employee under a Pseudonym – High Level – QSCD SmartCard/Token
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.1 [Camerfirma] 1.3.6.1.4.1.17326.99.18.1 2.16.724.1.3.5.7.1 [national regulations - Public Administrations - public employee - high level] 0.4.0.194112.1.2 [ETSI EN 319 411-2 – QCP-n-qscd]	Qualified Certificate for Signature for a Public Employee – High Level – QSCD Cloud
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.1 [Camerfirma] 1.3.6.1.4.1.17326.99.18.1 [Camerfirma] 2.16.724.1.3.5.4.1 [national regulations - Public Administrations - public employee under a pseudonym - high level] 0.4.0.194112.1.2 [ETSI EN 319 411-2 – QCP-n-qscd]	Qualified Certificate for Signature for a Public Employee under a Pseudonym – High Level – QSCD Cloud
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.2 [Camerfirma] 2.16.724.1.3.5.7.1 [national regulations - Public Administrations - public employee - high level] 0.4.0.2042.1.2 [ETSI EN 319 411-1 – NCP+]	Non-Qualified Certificate for Authentication for a Public Employee – High Level – SmartCard/Token
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.2 [Camerfirma] 2.16.724.1.3.5.4.1 [national regulations - Public Administrations - public employee under a pseudonym - high level] 0.4.0.2042.1.2 [ETSI EN 319 411-1 – NCP+]	Non-Qualified Certificate for Authentication for a Public Employee under a Pseudonym – High Level – SmartCard/Token
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.2 [Camerfirma] 1.3.6.1.4.1.17326.99.18.1 [Camerfirma] 2.16.724.1.3.5.7.1 [national regulations - Public Administrations - public employee - high level] 0.4.0.2042.1.2 [ETSI EN 319 411-1 – NCP+]	Non-Qualified Certificate for Authentication for a Public Employee – High Level – Cloud
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.2 [Camerfirma]	Non-Qualified Certificate for Authentication for a Public Employee under a Pseudonym –

1.3.6.1.4.1.17326.99.18.1 [Camerfirma] 2.16.724.1.3.5.4.1 [national regulations - Public Administrations - public employee under a pseudonym - high level] 0.4.0.2042.1.2 [ETSI EN 319 411-1 – NCP+]	High Level – Cloud
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.3 [Camerfirma] 2.16.724.1.3.5.7.1 [national regulations - Public Administrations - public employee - high level]	Non-Qualified Certificate for Encipherment for a Public Employee – High Level – SmartCard/Token.
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.3 [Camerfirma] 2.16.724.1.3.5.4.1 [national regulations - Public Administrations - public employee under a pseudonym - high level]	Non-Qualified Certificate for Encipherment for a Public Employee under a Pseudonym – High Level – SmartCard/Token
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.3 [Camerfirma] 1.3.6.1.4.1.17326.99.18.1 [Camerfirma] 2.16.724.1.3.5.7.1 [national regulations - Public Administrations - public employee - high level]	Non-Qualified Certificate for Encipherment for a Public Employee – High Level – Cloud
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.3 [Camerfirma] 1.3.6.1.4.1.17326.99.18.1 [Camerfirma] 2.16.724.1.3.5.4.1 [national regulations - Public Administrations - public employee under a pseudonym - high level]	Non-Qualified Certificate for Encipherment for a Public Employee under a Pseudonym – High Level – Cloud.
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.4 [Camerfirma] 2.16.724.1.3.5.7.2 [national regulations - Public Administrations - public employee - medium level] 0.4.0.194112.1.2 [ETSI EN 319 411-2 – QCP-n-qscd]	Qualified Certificate for a Public Employee – Medium Level – QSCD SmartCard/Token
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.4 [Camerfirma] 2.16.724.1.3.5.4.2 [national regulations - Public Administrations - public employee under a pseudonym - medium level] 0.4.0.194112.1.2 [ETSI EN 319 411-2 – QCP-n-qscd]	Qualified Certificate for a Public Employee under a Pseudonym – Medium Level – QSCD SmartCard/Token
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.4 [Camerfirma] 2.16.724.1.3.5.7.2 [national regulations - Public Administrations - public employee - medium level] 0.4.0.194112.1.0 [ETSI EN 319 411-2 – QCP-n]	Qualified Certificate for a Public Employee – Medium Level – Non-QSCD

1.3.6.1.4.1.17326.10.16.1.5.1.3.4.4 [Camerfirma] 2.16.724.1.3.5.4.2 [national regulations - Public Administrations - public employee under a pseudonym - medium level] 0.4.0.194112.1.0 [ETSI EN 319 411-2 – QCP-n]	Qualified Certificate for a Public Employee under a Pseudonym – Medium Level – Non-QSCD
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.4 [Camerfirma] 1.3.6.1.4.1.17326.99.18.1 [Camerfirma] 2.16.724.1.3.5.7.2 [national regulations - Public Administrations - public employee - medium level] 0.4.0.194112.1.2 [ETSI EN 319 411-2 – QCP-n-qscd]	Qualified Certificate for a Public Employee – Medium Level – QSCD Cloud
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.4 1.3.6.1.4.1.17326.99.18.1 [Camerfirma] 2.16.724.1.3.5.4.2 [national regulations - Public Administrations - public employee under a pseudonym - medium level] 0.4.0.194112.1.2 [ETSI EN 319 411-2 – QCP-n-qscd]	Qualified Certificate for a Public Employee under a Pseudonym – Medium Level – QSCD Cloud
AC CAMERFIRMA FOR LEGAL PERSONS – 2016	
2.5.29.32.0 [anyPolicy]	
1.3.6.1.4.1.17326.10.16.2.1.1 [Camerfirma] 0.4.0.194112.1.3 [ETSI EN 319 411-2 – QCP-l-qscd]	Qualified Certificate for Electronic Seal – QSCD SmartCard/Token
1.3.6.1.4.1.17326.10.16.2.1.2 [Camerfirma] 0.4.0.194112.1.1 [ETSI EN 319 411-2 – QCP-l]	Qualified Certificate for Electronic Seal – Non-QSCD
1.3.6.1.4.1.17326.10.16.2.2.1.3.3.1 [Camerfirma] 0.4.0.194112.1.3 [ETSI EN 319 411-2 – QCP-l-qscd] 2.16.724.1.3.5.6.1 [national regulations - Public Administrations - electronic seal - high level]	Qualified Certificate for Electronic Seal for Public Administrations – High Level – QSCD SmartCard/Token
1.3.6.1.4.1.17326.10.16.2.2.1.4.3.1 [Camerfirma] 0.4.0.194112.1.1 [ETSI EN 319 411-2 – QCP-l] 2.16.724.1.3.5.6.2 [national regulations - Public Administrations - electronic seal - medium level]	Qualified Certificate for Electronic Seal for Public Administrations – Medium Level – Non-QSCD
AC CAMERFIRMA TSA – 2016	
Does not issue new certificates	
2.5.29.32.0 [anyPolicy]	

1.3.6.1.4.1.17326.10.16.5.1.1 [Camerfirma]	TSU Qualified Certificate – QSCD HSM
0.4.0.194112.1.3 [ETSI EN 319 411-2 – QCP-I-qscd]	
<u>Chambers of Commerce Root – 2008</u>	
2.5.29.32.0 [anyPolicy] (certificates SHA-1 and SHA-256)	
Camerfirma TSA II – 2014	
2.5.29.32.0 [anyPolicy]	
1.3.6.1.4.1.17326.10.13.1.3 [Camerfirma]	TSU Non-Qualified Certificate – HSM
Camerfirma Codesign II – 2014	
2.5.29.32.0 [anyPolicy]	
1.3.6.1.4.1.17326.10.12.2 [Camerfirma]	Code Signing Non-Qualified Certificate
Camerfirma Corporate Server II – 2015	
2.5.29.32.0 [anyPolicy]	
1.3.6.1.4.1.17326.10.11.3.1.1 [Camerfirma]	Non-Qualified Certificate for Electronic Seal – P12
1.3.6.1.4.1.17326.10.11.3.1.2 [Camerfirma]	Non-Qualified Certificate for Electronic Seal – P10
Camerfirma AAPP II – 2014	
Does not issue new certificates	
2.5.29.32.0 [anyPolicy]	
1.3.6.1.4.1.17326.1.3.3.2 [Camerfirma]	Non-Qualified Certificate for Electronic Seal for Public Administrations
1.3.6.1.4.1.17326.1.3.4.4 [Camerfirma]	Non-Qualified Certificate for Personnel for Public Administrations
CAs under this CPS	
1.3.6.1.4.1.17326.10.9.8 [Camerfirma]	Non-Qualified OCSP Certificate - HSM

* Each of the CAs aforementioned issues its corresponding OCSP certificate

The following sections describe the Subordinate CAs under this CPS within the CHAMBERS OF COMMERCE ROOT hierarchies, and, where applicable, the corresponding CPs for active issued certificates, except the CP of OCSP certificates (see section 1.3.1.5).

1.3.1.1.1 AC CAMERFIRMA FOR NATURAL PERSONS - 2016

This Subordinate CA issues qualified and non-qualified certificates to natural persons within the EU, in accordance with the requirements of eIDAS Regulation and Law 6/2020.

The identification details for this Subordinate CA certificate (issued by the Root CA of the CHAMBERS OF COMMERCE ROOT – 2016 hierarchy) are:

CN: AC CAMERFIRMA FOR NATURAL PERSONS - 2016

Valid from (UTC time): 14/04/2016 08:48:09

Valid until (UTC time): 09/03/2040 08:48:09

Serial Number: 5151 4CB4 4FA4 54F5

X509v3 Subject Key Identifier: 70B8 F824 C751 CACE 2280 9208 C9C0 682F C147 5851

Hash SHA-1: 171A 2ADB 87CA 5927 047A 6E76 9757 3877 B5D6 02E5

Hash SHA-256: EEDD 457A F135 3D76 F48E 7C61 23F3 9140 E5F9 A069 CA51 B43E EA86 15C9
CECO D4BB

The CPs of the active certificates issued by this Subordinate CA, except the PC of OCSP certificates (see section 1.3.1.5), are:

1.3.1.1.1 QUALIFIED CITIZEN CERTIFICATE

This qualified certificate identifies a natural person (Subject/Signatory) only to act on his/her own behalf (with no attributes).

1.3.1.1.2 QUALIFIED CORPORATE CERTIFICATE / QUALIFIED CERTIFICATE FOR A SELF-EMPLOYED / QUALIFIED CERTIFICATE FOR A CHARTERED SELF-EMPLOYED

1.3.1.1.2.1 Qualified Corporate Certificate

This qualified certificate identifies a natural person (Subject/Signatory) and determines, as specific attributes, his/her relationship (labor, commercial, institution, etc.) with an Entity.

1.3.1.1.2.2 Qualified Certificate for a Self-employed

This qualified certificate identifies a natural person (Subject/Signatory) and determines, as specific attributes, his/her self-employed status, his/her economic activity, and, if applicable, the registered trade name under which the self-employed person carries out his/her profession.

1.3.1.1.2.3 Qualified Certificate for a Chartered Self-employed

This qualified certificate identifies a natural person (Subject/Signatory) and determines, as specific

attributes, his/her self-employed status, his/her professional activity, his/her registered professional status, and, if applicable, the registered trade name under which the self-employed person carries out their profession.

1.3.1.1.3 QUALIFIED CERTIFICATES FOR A REPRESENTATIVE

1.3.1.1.3.1 Qualified Certificate for a Legal Representative of a Legal/Non-Legal Entity

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

It is aimed at legal representatives of Legal Entities (Sole Administrator, Joint Administrator, Managing Director, etc.), legal representatives of Non-Legal Entities (Sole Administrator, Joint Administrator, Director/Manager, President of Property Owners, etc.), and representatives with very broad powers of representation of Legal Entities (similar to those of a legal representative) that allows them to act both in the field of the Entity's relations and procedures with the Public Administrations (authentication and signature uses) and in the field of contracting goods or services relating to the ordinary business of the Entity (signature uses).

The jointly legal representatives and the jointly representatives who want to request this certificate must hold powers that include the joint power to represent the Legal or Non-Legal Entity to carry out relations and procedures with Public Administrations.

In any case, the certificate Subject is responsible for using it in accordance with its powers and the Relying Party is responsible for verifying its content and scope.

The certificates issued under these CPs are in accordance with the Spanish national regulations for certificate profiles for a natural person representative of a legal entity and for a natural person representative of a non-legal entity established in section 14.1 of the document "Electronic certificate profiles" of the Sub-directorate General for Information, Documentation and Publications of the Ministry of Finance and Public Administrations.

1.3.1.1.3.2 Qualified Certificate for a Voluntary Representative of a Legal/Non-Legal Entity before the Public Administrations

This qualified certificate identifies a natural person (Subject/Signatory) and determines, as specific attributes, his/her capability to represent a Legal or Non-Legal Entity in the field of the Entity's relations and procedures with Public Administrations (authentication and signature uses).

It is aimed at representatives with a general power or a specific power which includes faculties that enable them to perform, on behalf of the Legal or Non-Legal Entity, actions and procedures with Public Administrations that require the use of electronic signature or electronic certificate.

The jointly representatives who want to request this certificate must hold powers that include the

joint power to represent the Legal or Non-legal Entity to carry out relations and procedures with Public Administrations. Alternatively, they can provide a specific power or a reliable document signed by all the representatives in favour of one of them.

In any case, the certificate Subject is responsible for using it in accordance with its powers and the Relying Party is responsible for verifying its content and scope.

The certificates issued under these CPs are in accordance with the Spanish national regulations for certificate profiles for a natural person representative of a legal entity and for a natural person representative of a non-legal entity established in section 14.1 of the document "Electronic certificate profiles" of the Sub-directorate General for Information, Documentation and Publications of the Ministry of Finance and Public Administrations.

1.3.1.1.1.3.3 Qualified Certificate for a Special Representative of a Legal/Non-Legal Entity

This qualified certificate identifies a natural person (Subject/Signatory) and determines, as specific attributes, his/her capability to act on behalf of a Legal or Non-Legal Entity only for certain powers framed in his/her function/department in the Entity (signature uses for private documents in the ordinary commercial activity of the Entity).

This certificate is not valid for authentication or signature uses on behalf of a Legal or Non-Legal Entity on Public Administration platforms, because of the implicit limitation of the powers whose accurate scope the Relying Party cannot know.

The jointly representatives who want to request this certificate must hold powers that include the corresponding powers framed in his/her function/department in the Entity. Alternatively, they can provide a specific power or a reliable document signed by all the representatives in favour of one of them.

In any case, the certificate Subject is responsible for using it in accordance with its powers and the Relying Party is responsible for verifying its content and scope.

1.3.1.1.1.4 CERTIFICATES FOR A PUBLIC EMPLOYEE WITH/WITHOUT A PSEUDONYM

These certificates identify a natural person (Subject/Signatory) as a public employee.

The qualified certificates issued under these CPs can be used by the electronic signature systems of the personnel in the service of the Public Administrations, in accordance with the provisions of article 43 of the Spanish Law 40/2015, of 1 October, on the Legal Regime of the Public Sector.

The certificates issued under these CPs are in accordance with the Spanish national regulations for certificate profiles for a public employee and for a public employee with pseudonym established in sections 10 and 11 of the document "Electronic certificate profiles" of the Sub-directorate General for Information, Documentation and Publications of the Ministry of Finance and Public Administrations, at their high and medium/substantial levels.

1.3.1.1.2 AC CAMERFIRMA FOR LEGAL PERSONS - 2016

This Subordinate CA issues qualified certificates to legal persons within the EU, in accordance with the requirements of eIDAS Regulation and Law 6/2020.

The identification details for this Subordinate CA certificate (issued by the Root CA of the CHAMBERS OF COMMERCE ROOT – 2016 hierarchy) are:

CN: AC CAMERFIRMA FOR LEGAL PERSONS - 2016

Valid from (UTC time): 14/04/2016 08:33:07

Valid until (UTC time): 09/03/2040 08:33:07

Serial Number: 54B1 6EE1 1124 5A42

X509v3 Subject Key Identifier: C327 8593 D72F 96C5 1BAC 7633 D986 A24A 7D68 1442

Hash SHA-1: EBEE 22EB A7AC 3F68 0175 1756 2414 61D7 D749 E730

Hash SHA-256: 3A80 6626 6D28 BD28 CCD0 F564 C8FB C121 9B4F FAE4 03E0 1E50 39D3 0F24 00F0 EB09

The CPs of the active certificates issued by this Subordinate CA, except the PC of OCSP certificates (see section 1.3.1.5), are:

1.3.1.1.2.1 QUALIFIED CERTIFICATE FOR ELECTRONIC SEAL

This qualified certificate identifies a legal person (Subject / Creator of a Seal).

The Applicant for this certificate must have powers of representation that enable him/her to apply for the certificate on behalf of the legal person to which the certificate is issued.

The use of the private key associated with this certificate provides integrity and authenticity to the documents and transactions to which it is applied.

This certificate can be associated with a private key activated by a machine or application, to allow the operations that use it to be carried out automatically and unassisted. It is also allowed as a client machine or application identification element in secure electronic communication protocols TLS.

1.3.1.1.2.2 QUALIFIED CERTIFICATE FOR ELECTRONIC SEAL FOR PUBLIC ADMINISTRATIONS

This qualified certificate identifies a legal person of the Public Administration type (Subject / Creator of a Seal), in accordance with the provisions of article 40 of the Spanish Law 40/2015, of 1 October, on the Legal Regime of the Public Sector.

The Applicant for this certificate must have powers of representation that enable him/her to apply for the certificate on behalf of the Public Administration to which the certificate is issued.

The use of the private key associated with this certificate provides integrity and authenticity to the documents and transactions to which it is applied.

This certificate can be associated with a private key activated by a machine or application, to allow the operations that use it to be carried out automatically and unassisted. It is also allowed as a client machine or application identification element in secure electronic communication protocols TLS.

The certificates issued under these CPs can be used by the signature systems for automated administrative processing, in accordance with the provisions of article 42 of the Spanish Law 40/2015, of 1 October, on the Legal Regime of the Public Sector.

The certificates issued under these CPs are in accordance with the Spanish national regulations for certificate profile for electronic seal established in section 9 of the document "Electronic certificate profiles" of the Sub-directorate General for Information, Documentation and Publications of the Ministry of Finance and Public Administrations, at their high and medium/substantial levels.

1.3.1.1.3 AC CAMERFIRMA TSA - 2016, CAMERFIRMA TSA II - 2014

These Subordinate CAs issue certificates to legal persons for digital signing of time-stamps.

A time-stamp 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.

These Subordinate CAs issue certificates to intermediate entities called "Time-Stamping Units" (TSUs). These TSUs ultimately issue the time-stamps on receiving a standard request by the IETF RFC 3161 specifications. Each of these TSUs can be associated either with the service's specific technical features or exclusive client use.

TSU certificates can be issued to Camerfirma and other companies and entities (legal persons) residing inside or outside of Spanish territory.

Camerfirma issues TSU certificates on equipment accredited by Camerfirma. The accredited equipment may be located on Camerfirma's premises or on the premises of the client through the signature of an affidavit of compliance with the requirements associated with the use of the TSU certificate and equipment.

Camerfirma also issues TSU certificates on third-party platforms as long as the keys are generated and stored in an HSM in accordance with the requirements of the corresponding CP. The client must submit a key generation signed report compliant with these requirements. This report is first reviewed by Camerfirma technical personnel before validation is given.

The identification details for these Subordinate CAs certificates certificate (issued by the Root CA of the Chambers of Commerce Root – 2008 hierarchy) are:

- **AC CAMERFIRMA TSA – 2016** (issued by the Root CA of the CHAMBERS OF COMMERCE ROOT – 2016 hierarchy)
CN: AC CAMERFIRMA TSA - 2016
Valid from (UTC time): 14/04/2016 10:42:09
Valid until (UTC time): 09/03/2040 10:42:09

Serial Number: 15B7 A58A 54FF 0282

X509v3 Subject Key Identifier: 1E6D B5C6 3FEF 9255 5E37 FADB FD10 AABA D93B 4E2C

Hash SHA-1: 907F 23C8 E03C 7837 436E 1FB0 3743 7751 75B7 02E6

Hash SHA-256: BAAE 2C63 3885 7D50 200F 6F73 DD45 E65A A2D8 95BE D467 5B6E 396B 7222 E018 A9B8

- **Camerfirma TSA II – 2014** (issued by the Root CA of the Chambers of Commerce Root – 2008 hierarchy)

CN: Camerfirma TSA II - 2014

Valid from (UTC time): 16/12/2014 16:45:33

Valid until (UTC time): 15/12/2037 16:45:33

Serial Number: 25A4 54BC 3455 1238

X509v3 Subject Key Identifier: 17C5 40BC 2AF8 45B8 AB33 BFF8 6F49 6CF6 17CA B7D4

Hash SHA-1: 19EB DCED EDEB C925 1F3A 098F F4C9 51AE 5552 48B1

Hash SHA-256: 6569 5D50 0117 FD72 70F1 027E D121 F059 4267 0075 461D 337E EEC7 F6A5 B757 A47A

The Subordinate CA AC CA CAMERFIRMA TSA – 2016 does not issue new certificates.

The CPs of the active certificates issued by these Subordinate CAs, except the PC of OCSP certificates (see section 1.3.1.5), are:

1.3.1.1.3.1 TSU QUALIFIED CERTIFICATE

This qualified certificate identifies a legal person (Subject / Creator of a Seal).

The Applicant for this certificate must have powers of representation that enable him/her to apply for the certificate on behalf of the legal person to which the certificate is issued.

This certificate can be used for digital signing of time-stamps.

The keys of this certificate are generated and stored in an HSM QSCD, in accordance with the requirements set out in ETSI EN 319 421.

1.3.1.1.3.2 TSU NON-QUALIFIED CERTIFICATE

This non-qualified certificate identifies a legal person (Subject / Creator of a Seal).

The Applicant for this certificate must have powers of representation that enable him/her to apply for the certificate on behalf of the legal person to which the certificate is issued.

This certificate can be used for digital signing of time-stamps.

The keys of this certificate are generated and stored in an HSM FIPS 140-2 level 3 or FIPS 140-3

level 3 or CC EAL 4 or higher, Non-QSCD or QSCD, in accordance with the requirements set out in ETSI EN 319 421.

1.3.1.1.4 CAMERFIRMA CODESIGN II – 2014

This Subordinate CA issues certificates to legal persons for code signing.

The identification details for this Subordinate CA certificate (issued by the Root CA of the Chambers of Commerce Root – 2008 hierarchy) are:

CN: Camerfirma Codesign II - 2014

Valid from (UTC time): 16/12/2014 12:25:43

Valid until (UTC time): 15/12/2037 12:25:43

Serial Number: 6451 2A01 FB00 554A

X509v3 Subject Key Identifier: C4A3 D3EA 633D 4961 DA91 C919 D91B 3335 7875 389F

Hash SHA-1: 247D 88C9 5017 7261 1BB1 5A35 61A7 72DA A16F 2950

Hash SHA-256: 3B0B 2D29 9AF7 74D6 C332 B2BF ABB4 5F44 D866 432B 9552 EA09 4D52 9B6E D125 048B

The CPs of the active certificates issued by this Subordinate CA, except the PC of OCSP certificates (see section 1.3.1.5), are:

1.3.1.1.4.1 CODE SIGNING NON-QUALIFIED CERTIFICATE

This non-qualified certificate identifies a legal person (Subject / Creator of a Seal).

The Applicant for this certificate must have powers of representation that enable him/her to apply for the certificate on behalf of the legal person to which the certificate is issued.

This certificate allows developers to apply a digital signature on code (ActiveX, java applets, macros for Microsoft Office, etc.) thus establishing, in this way, on said code guarantees of integrity and authenticity.

1.3.1.1.5 CAMERFIRMA CORPORATE SERVER II – 2015

This Subordinate CA issues certificates to legal persons.

The identification details for this Subordinate CA certificate (issued by the Root CA of the Chambers of Commerce Root – 2008 hierarchy) are:

CN: Camerfirma Corporate Server II - 2015

Valid from (UTC time): 15/01/2015 09:21:16

Valid until (UTC time): 15/12/2037 09:21:16

Serial Number: 621F F31C 489B A136

X509v3 Subject Key Identifier: 63E9 F0F0 5600 6865 B021 6C0E 5CD7 1908 9D08 3465

Hash SHA-1: FE72 7A78 EA0C 0335 CDDA 9C2E D75F D4D4 6F35 C2EF

Hash SHA-256: 66EA E270 9B54 CDD1 6931 77B1 332F F036 CDD0 F723 DB30 39ED 3115 55A6 CBF5 FF3E

The CPs of the active certificates issued by this Subordinate CA, except the PC of OCSP certificates (see section 1.3.1.5), are:

1.3.1.1.5.1 NON-QUALIFIED CERTIFICATE FOR ELECTRONIC SEAL

This non-qualified certificate identifies a legal person (Subject / Creator of a Seal).

The Applicant for this certificate must have powers of representation that enable him/her to apply for the certificate on behalf of the legal person to which the certificate is issued.

The use of the private key associated with this certificate provides integrity and authenticity to the documents and transactions to which it is applied.

This certificate can be associated with a private key activated by a machine or application, to allow the operations that use it to be carried out automatically and unassisted. It is also allowed as a client machine or application identification element in secure electronic communication protocols TLS.

1.3.1.1.6 CAMERFIRMA AAPP II – 2014

This Subordinate CA issues certificates to natural persons and legal persons of Public Administrations.

This Subordinate CA does not issue new certificates.

The identification details for this Subordinate CA certificate (issued by the Root CA of the Chambers of Commerce Root – 2008 hierarchy) are:

CN: Camerfirma AAPP II - 2014

Valid from (UTC time): 16/12/2014 11:59:01

Valid until (UTC time): 15/12/2037 11:59:01

Serial Number: 1548 D054 B8A8 42BA

X509v3 Subject Key Identifier: 5DA1 55A4 DC4A AC83 11F9 AA38 E5F7 684A FE15 154C

Hash SHA-1: E95E CC41 4D56 452A E354 09AC D23F 34A2 7BDB D26E

Hash SHA-256: 7239 D2F7 70FA FF3B 1CF8 BE2A 05EC 03ED EAAC 053B 554F 90D3 6921 155B A805 1981

The CPs of the active certificates issued by this Subordinate CA, except the PC of OCSP certificates

(see section 1.3.1.5), are:

1.3.1.1.6.1 NON-QUALIFIED CERTIFICATE FOR ELECTRONIC SEAL FOR PUBLIC ADMINISTRATIONS

This non-qualified certificate identifies a legal person of the Public Administration type (Subject / Creator of a Seal).

The Applicant for this certificate must have powers of representation that enable him/her to apply for the certificate on behalf of the legal person to which the certificate is issued.

The use of the private key associated with this certificate provides integrity and authenticity to the documents and transactions to which it is applied.

This certificate can be associated with a private key activated by a machine or application, to allow the operations that use it to be carried out automatically and unassisted. It is also allowed as a client machine or application identification element in secure electronic communication protocols TLS.

1.3.1.1.6.2 NON-QUALIFIED CERTIFICATE FOR PERSONNEL FOR PUBLIC ADMINISTRATIONS

This non-qualified certificate identifies a natural person (Subject/Signatory) as a public employee.

This certificate allows the uses of authentication, signature and encryption.

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 ATTRIBUTE *ORGANIZATION* OF THE FIELD *SUBJECT* OF THE CORRESPONDING ROOT CAS CERTIFICATES.

These hierarchies are designed for issuing certificates for specific projects with specific entity or entities. They are therefore open hierarchies in which certificates and their management are adapted to specific project needs. In this sense, unlike the CHAMBERS OF COMMERCE ROOT hierarchies, the end entities certificates issued under these hierarchies and their corresponding CAs and RAs have no territorial limitations.

The GLOBAL CHAMBERSIGN ROOT hierarchies organize the issuance of certificates by Subordinate CAs established in different territories by means of Subordinate CAs owned by Camerfirma created specifically for issuing certificates in these territories, thus allowing better adaptation to the corresponding legal and regulatory frameworks.

Under these hierarchies, certificates can be issued by Subordinate CAs established anywhere in the world, provided that CAs and RAs meet the requirements set by Camerfirma, always subject to the applicable laws and regulations in force.

The Subordinate CAs that issue certificates under these hierarchies may be owned by Camerfirma or by other TSPs. All the CAs that operate under these hierarchies do so from infrastructures

technically controlled by Camerfirma.

The identification details for the active Root CAs certificates of these hierarchies are:

- **GLOBAL CHAMBERSIGN ROOT – 2016**

CN: GLOBAL CHAMBERSIGN ROOT - 2016

Valid from (UTC time): 14/04/2016 07:50:06

Valid until (UTC time): 08/04/2040 07:50:06

Serial Number: 2DD2 2E50 30A6 5E13

X509v3 Subject Key Identifier: E89B CD7E 8662 9B7A 4D8C 0097 3985 CF1C 7890 703A

Hash SHA-1: 1139 A49E 8484 AAF2 D90D 985E C474 1A65 DD5D 94E2

Hash SHA-256: C1D8 0CE4 74A5 1128 B77E 794A 98AA 2D62 A022 5DA3 F419 E5C7 ED73
DFBF 660E 7109

The following table shows the scheme of active Root CAs and Subordinate CAs under these hierarchies, including, where applicable, the respective OIDs in the *Certificate Policies* extension of the certificates of each CA and of the different types of active certificates issued by each Subordinate CA under this CPS.

<u>GLOBAL CHAMBERSIGN ROOT – 2016</u>
AC CAMERFIRMA COLOMBIA – 2016 Issues Subordinate CA certificates 2.5.29.32.0 [anyPolicy]
CAMERFIRMA COLOMBIA SAS CERTIFICADOS – 001 (Subordinate CA of AC CAMERFIRMA COLOMBIA – 2016) Owned by CAMERFIRMA COLOMBIA SAS and it is governed by its own CPS and CPs 1.3.6.1.4.1.17326.20.10.0 [Camerfirma]
CAMERFIRMA COLOMBIA SAS CERTIFICADOS – 002 (Subordinate CA of AC CAMERFIRMA COLOMBIA – 2016) Owned by CAMERFIRMA COLOMBIA SAS and it is governed by its own CPS and CPs 1.3.6.1.4.1.17326.20.10.0 [Camerfirma]
AC CAMERFIRMA PERÚ – 2016 Issues Subordinate CA certificates 2.5.29.32.0 [anyPolicy]
AC CAMERFIRMA PERÚ CERTIFICADOS – 2016 (Subordinate CA of AC CAMERFIRMA PERÚ – 2016)

Owned by CAMERFIRMA PERÚ S.A.C and it is governed by this CPS and its own CPS and CPs 2.5.29.32.0 [anyPolicy]	
AC CAMERFIRMA PERÚ CERTIFICADOS – 2023 (Subordinate CA of AC CAMERFIRMA PERÚ – 2016)	
Owned by CAMERFIRMA PERÚ S.A.C and it is governed by this CPS and its own CPS and CPs 2.5.29.32.0 [anyPolicy]	
CAs under this CPS	
1.3.6.1.4.1.17326.10.9.8 [Camerfirma]	Non-Qualified OCSP Certificate - HSM

* Each of the CAs aforementioned issues its corresponding OCSP certificate.

The following sections describe the Subordinate CAs under this CPS within the CHAMBERSIGN GLOBAL ROOT hierarchies, and, where applicable, the corresponding CPs for active issued certificates, except the CP of OCSP certificates (see section 1.3.1.5).

1.3.1.2.1 AC CAMERFIRMA COLOMBIA – 2016

This Subordinate CA issues Subordinate CA certificates within the geographical scope of the Republic of Colombia.

The identification details for this Subordinate CA certificate (issued by the Root CA of the Chambers of GLOBAL CHAMBERSIGN ROOT– 2016 hierarchy) are:

CN: AC CAMERFIRMA COLOMBIA - 2016

Valid from (UTC time): 14/04/2016 11:10:07

Valid until (UTC time): 09/03/2040 11:10:07

Serial Number: 3F00 A087 126F 41D2

X509v3 Subject Key Identifier: 8994 7ACB 691B 9E30 5624 C0D4 12BF 5E09 17D7 279C

Hash SHA-1: 394E 613C 7852 7BF4 FF42 3195 9FC4 7ECC 9762 E6E4

Hash SHA-256: 8234 8E56 FF76 5293 EBE7 E2A5 B7B0 57F5 C131 C3BC 68DB E7DB 4353 1F40 C76A 3B2D

1.3.1.2.2 AC CAMERFIRMA PERÚ – 2016

This Subordinate CA issues Subordinate CA certificates within the geographical scope of the Republic of Peru and more generally of LATAM countries which can recognize its validity.

The identification details for this Subordinate CA certificate (issued by the Root CA of the Chambers of GLOBAL CHAMBERSIGN ROOT– 2016 hierarchy) are:

CN: AC CAMERFIRMA PERÚ - 2016

Valid from (UTC time): 11/10/2016 08:37:59

Valid until (UTC time): 10/03/2040 08:37:59

Serial Number: 26F4 AA13 F056 0872

X509v3 Subject Key Identifier: B76A 026D 2CD9 B036 B32B 6C05 AA34 5E06 EDB2 B99B

Hash SHA-1: 45A2 5644 3A16 31C8 51A1 1563 10F5 F385 736B D2C5

Hash SHA-256: 71A0 214D 43E5 B359 6DDB 36AF 8459 E9E5 79AE 929B 800D 94A9 E3F6 71E9
F431 C4F3

1.3.1.3 CAMERFIRMA ROOT 2021 HIERARCHY

Certificates issued under this hierarchy and their corresponding CAs and RAs have no territorial limitations.

Under this hierarchy, certificates can be issued by Subordinate CAs established anywhere in the world, provided that CAs and RAs meet the requirements set by Camerfirma, always subject to the applicable laws and regulations in force.

The Subordinate CAs that issue certificates under this hierarchy may be owned by Camerfirma or by other TSP. All the CAs that operate under this hierarchy do so from infrastructures technically controlled by Camerfirma.

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

CN: CAMERFIRMA ROOT 2021

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

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

Serial Number: 3461 2CA9 B6C3 7A12 FE65 50A0 6B28 EEEC EEBA F3E4

X509v3 Subject Key Identifier: 5111 327A 10D0 D88C 4C09 8497 B1A9 3EB2 54BA 87C9

Hash SHA-1: 339F 6EF0 37AA EEBA A0CE 5480 0602 DDFB 186C 1CEE

Hash SHA-256: ADFC 9410 EE0D 1091 EEFD 5CDD FAE5 651E 3B1D 66B6 9C0D ABC5 9E33 91B3
585A 538E

The following table shows the scheme of active Root CA and Subordinate CAs under this hierarchy, including, where applicable, the respective OIDs in the *Certificate Policies* extension of the certificates of each CA and of the different types of active certificates issued by each Subordinate CA under this CPS.

CAMERFIRMA ROOT 2021

AC CAMERFIRMA QUALIFIED CERTIFICATES – 2021

1.3.6.1.4.1.17326.10.21.1.1.1 [Camerfirma] 0.4.0.194112.1.2 [ETSI EN 319 411-2 - QCP-n-qscd]	Qualified Citizen Certificate - QSCD SmartCard/Token
1.3.6.1.4.1.17326.10.21.1.1.3 [Camerfirma] 0.4.0.194112.1.2 [ETSI EN 319 411-2 - QCP-n-qscd]	Qualified Citizen Certificate - QSCD Cloud
1.3.6.1.4.1.17326.10.21.1.2.1 [Camerfirma] 0.4.0.194112.1.2 [ETSI EN 319 411-2 - QCP-n-qscd]	Qualified Corporate Certificate - QSCD SmartCard/Token
1.3.6.1.4.1.17326.10.21.1.2.3 [Camerfirma] 0.4.0.194112.1.2 [ETSI EN 319 411-2 - QCP-n-qscd]	Qualified Corporate Certificate - QSCD Cloud
1.3.6.1.4.1.17326.10.21.1.3.1 [Camerfirma] 2.21.724.1.3.5.8 [national regulations - representative of a legal person] 0.4.0.194112.1.2 [ETSI EN 319 411-2 – QCP-n-qscd]	Qualified Certificate for a Legal Representative of a Legal Entity – QSCD SmartCard/Token
1.3.6.1.4.1.17326.10.21.1.3.3 [Camerfirma] 2.21.724.1.3.5.8 [national regulations - representative of a legal person] 0.4.0.194112.1.2 [ETSI EN 319 411-2 - QCP-n-qscd]	Qualified Certificate for a Legal Representative of a Legal Entity - QSCD Cloud
1.3.6.1.4.1.17326.10.21.1.4.1 [Camerfirma] 2.21.724.1.3.5.9 [national regulations - representative of a non-legal entity] 0.4.0.194112.1.2 [ETSI EN 319 411-2 - QCP-n-qscd]	Qualified Certificate for a Legal Representative of a Non-Legal Entity - QSCD SmartCard/Token
1.3.6.1.4.1.17326.10.21.1.4.3 [Camerfirma] 2.21.724.1.3.5.9 [national regulations - representative of a non-legal entity] 0.4.0.194112.1.2 [ETSI EN 319 411-2 - QCP-n-qscd]	Qualified Certificate for a Legal Representative of a Non-Legal Entity - QSCD Cloud
1.3.6.1.4.1.17326.10.21.1.5.1 [Camerfirma] 2.21.724.1.3.5.8 [national regulations - representative of a legal person] 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 – QSCD SmartCard/Token
1.3.6.1.4.1.17326.10.21.1.5.3 [Camerfirma] 2.21.724.1.3.5.8 [national regulations -	Qualified Certificate for a Voluntary Representative of a Legal Entity

representative of a legal person] 0.4.0.194112.1.2 [ETSI EN 319 411-2 - QCP-n-qscd]	before the Public Administrations - QSCD Cloud
1.3.6.1.4.1.17326.10.21.1.6.1 [Camerfirma] 2.21.724.1.3.5.9 [national regulations - representative of a non-legal entity] 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 - QSCD SmartCard/Token
1.3.6.1.4.1.17326.10.21.1.6.3 [Camerfirma] 2.21.724.1.3.5.9 [national regulations - representative of a non-legal entity] 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 - QSCD Cloud
1.3.6.1.4.1.17326.10.21.1.7.1 [Camerfirma] 0.4.0.194112.1.2 [ETSI EN 319 411-2 - QCP-n-qscd]	Qualified Certificate for a Special Representative of a Legal Entity - QSCD SmartCard/Token
1.3.6.1.4.1.17326.10.21.1.7.3 [Camerfirma] 0.4.0.194112.1.2 [ETSI EN 319 411-2 - QCP-n-qscd]	Qualified Certificate for a Special Representative of a Legal Entity - QSCD Cloud
1.3.6.1.4.1.17326.10.21.1.8.1 [Camerfirma] 0.4.0.194112.1.2 [ETSI EN 319 411-2 - QCP-n-qscd]	Qualified Certificate for a Special Representative of a Non-Legal Entity - QSCD SmartCard/Token
1.3.6.1.4.1.17326.10.21.1.8.3 [Camerfirma] 0.4.0.194112.1.2 [ETSI EN 319 411-2 - QCP-n-qscd]	Qualified Certificate for a Special Representative of a Non-Legal Entity - QSCD Cloud
CAs under this CPS	
1.3.6.1.4.1.17326.10.21.0.1 [Camerfirma]	Non-Qualified OCSP Certificate - HSM

* Each of the CAs aforementioned issues its corresponding OCSP certificate.

The following sections describe the Subordinate CAs under this CPS within the CAMERFIRMA ROOT 2021 hierarchy, and, where applicable, the corresponding CPs for active issued certificates, except the CP of OCSP certificates (see section 1.3.1.5).

1.3.1.3.1 AC CAMERFIRMA QUALIFIED CERTIFICATES - 2021

This Subordinate CA may issue qualified certificates to natural persons and legal persons (at present, only to natural persons) within the EU, in accordance with the requirements of eIDAS Regulation and Law 6/2020.

The identification details for this Subordinate CA certificate (issued by the Root CA of the

CAMERFIRMA ROOT 2021 hierarchy) are:

CN: AC CAMERFIRMA QUALIFIED CERTIFICATES - 2021

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

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

Serial Number: 1C20 0D92 1123 B898 380F C2B9 2419 BBA9 9B94 C2C2

X509v3 Subject Key Identifier: C76F 2DC4 108A 6EDD F311 6569 C64A 437B C30F 6814

Hash SHA-1: 2E0F 6F10 E614 5E50 57FC 03B2 53C5 006E E06D 19EE

Hash SHA-256: 4D18 7D4E 5BBA 7BBA D422 B75B EFB4 DCB2 179D 1CCD 115A 18D2 C835
OFFF AC31 6B34

The CPs of the active certificates issued by this Subordinate CA, except the PC of OCSP certificates (see section 1.3.1.5), are:

1.3.1.3.1.1 QUALIFIED CITIZEN CERTIFICATE

This qualified certificate identifies a natural person (Subject/Signatory) only to act on his/her own behalf (with no attributes).

1.3.1.3.1.2 QUALIFIED CORPORATE CERTIFICATE

This qualified certificate identifies a natural person (Subject/Signatory) and determines, as specific attributes, his/her relationship (labor, commercial, institution, etc.) with an Entity.

1.3.1.3.1.3 QUALIFIED CERTIFICATES FOR A REPRESENTATIVE

1.3.1.3.1.3.1 Qualified Certificate for a Legal Representative of a Legal Entity

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

It is aimed at legal representatives of Legal Entities (Sole Administrator, Joint Administrator, Managing Director, etc.), and representatives with very broad powers of representation of Legal Entities (similar to those of a legal representative) that allows them to act both in the field of the Entity's relations and procedures with the Public Administrations (authentication and signature uses) and in the field of contracting goods or services relating to the ordinary business of the Entity (signature uses).

The jointly legal representatives who want to request this certificate must hold powers that include the joint power to represent the Legal Entity to carry out relations and procedures with Public Administrations.

In any case, the certificate Subject is responsible for using it in accordance with its powers and the

Relying Party is responsible for verifying its content and scope.

The certificates issued under these CPs are in accordance with the Spanish national regulations for certificate profile for a natural person representative of a legal entity established in section 14.1 of the document "Electronic certificate profiles" of the Sub-directorate General for Information, Documentation and Publications of the Ministry of Finance and Public Administrations.

1.3.1.3.1.3.2 Qualified Certificate for a Legal Representative of a Non-Legal Entity

This qualified certificate identifies a natural person (Subject/Signatory) and determines, as specific attributes, his/her status as a legal representative c, with the capability to act on behalf of a Non-Legal Entity.

It is aimed at legal representatives of Non-Legal Entities (Sole Administrator, Joint Administrator, Director/Manager, President of Property Owners, etc.), and representatives with very broad powers of representation of Non-legal Entities (similar to those of a legal representative) that allows them to act both in the field of the Entity's relations and procedures with Public Administrations (authentication and signature uses) and in the field of contracting goods or services relating the ordinary business of the Entity (signature uses).

The jointly legal representatives and the jointly representatives who want to request this certificate must hold powers that include the joint power to represent the Non-Legal Entity to carry out relations and procedures with Public Administrations.

In any case, the certificate Subject is responsible for using it in accordance with its powers and the Relying Party responsible for verifying its content and scope.

The certificates issued under these CPs are in accordance with the Spanish national regulations for certificate profile for a natural person representative of a non-legal entity established in section 14.1 of the document "Electronic certificate profiles" of the Sub-directorate General for Information, Documentation and Publications of the Ministry of Finance and Public Administrations.

1.3.1.3.1.3.3 Qualified Certificate for a Voluntary Representative of a Legal Entity before the Public Administrations

This qualified certificate identifies a natural person (Subject/Signatory) and determines, as specific attributes, his/her capability to represent a Legal Entity in the field of the Entity's relations and procedures with Public Administrations (authentication and signature uses).

It is aimed at representatives with a general power or a specific power which includes faculties that enable them to perform, on behalf of the Legal Entity, actions and procedures with Public Administrations that require the use of electronic signature or electronic certificate.

The jointly representatives who want to request this certificate must hold powers that include the joint power to represent the Legal Entity to carry out relations and procedures with Public Administrations. Alternatively, they can provide a specific power or a reliable document signed by

all the representatives in favour of one of them.

In any case, the certificate Subject is responsible for using it in accordance with its powers and the Relying Party is responsible for verifying its content and scope.

The certificates issued under these CPs are in accordance with the Spanish national regulations for certificate profile for a natural person representative of a legal entity established in section 14.1 of the document "Electronic certificate profiles" of the Sub-directorate General for Information, Documentation and Publications of the Ministry of Finance and Public Administrations.

1.3.1.3.1.3.4 Qualified Certificate for a Voluntary Representative of a Non-Legal Entity before the Public Administrations

This qualified certificate identifies a natural person (Subject/Signatory) and determines, as specific attributes, his/her capability to represent a Non-Legal Entity in the field of the Entity's relations and procedures with Public Administrations (authentication and signature uses).

It is aimed at representatives with a general power or a specific power which includes faculties that enable them to perform, on behalf of the Non-Legal Entity, actions and procedures with Public Administrations that require the use of electronic signature or electronic certificate.

The jointly representatives who want to request this certificate must hold powers that include the joint power to represent the Non-Legal Entity to carry out relations and procedures with Public Administrations. Alternatively, they can provide a specific power or a reliable document signed by all the representatives in favour of one of them.

In any case, the certificate Subject is responsible for using it in accordance with its powers and the Relying Party is responsible for verifying its content and scope.

The certificates issued under these CPs are in accordance with the Spanish national regulations for certificate profile for a natural person representative of a non-legal entity established in section 14.1 of the document "Electronic certificate profiles" of the Sub-directorate General for Information, Documentation and Publications of the Ministry of Finance and Public Administrations.

1.3.1.3.1.3.5 Qualified Certificate for a Special Representative of a Legal Entity

This qualified certificate identifies a natural person (Subject/Signatory) and determines, as specific attributes, his/her capability to act on behalf of a Legal Entity only for certain powers framed in his/her function/department in the Entity (signature uses for private documents in the ordinary commercial activity of the Entity).

This certificate is not valid for authentication or signature uses on behalf of a Legal Entity on Public Administration platforms, because of the implicit limitation of the powers whose accurate scope the Relying Party cannot know.

The jointly representatives who want to request this certificate must hold powers that include the corresponding powers framed in his/her function/department in the Entity. Alternatively, they can

provide a specific power or a reliable document signed by all the representatives in favour of one of them.

In any case, the certificate Subject is responsible for using it in accordance with its powers and the Relying Party is responsible for verifying its content and scope.

1.3.1.3.1.3.6 Qualified Certificate for a Special Representative of a Non-Legal Entity

This qualified certificate identifies a natural person (Subject/Signatory) and determines, as specific attributes, his/her capability to act on behalf of a Non-Legal Entity only for certain powers framed in his/her function/department (signatures uses for private documents in the ordinary commercial activity of the Entity).

This certificate is not valid for authentication or signature uses on behalf of a Non-Legal Entity on Public Administration platforms, because of the implicit limitation of the powers whose accurate scope the Relying Party cannot know.

The jointly representatives who want to request this certificate must hold powers that include the corresponding powers framed in his/her function/department in the Entity. Alternatively, they can provide a specific power or a reliable document signed by all the representatives in favour of one of them.

In any case, the certificate Subject is responsible for using it in accordance with its powers and the Relying Party is responsible for verifying its content and scope.

1.3.1.4 INFOCERT-CAMERFIRMA ROOT 2024 HIERARCHY

Certificates issued under this hierarchy and their corresponding CAs and RAs have no territorial limitations.

Under this hierarchy, certificates can be issued by Subordinate CAs established anywhere in the world, provided that CAs and RAs meet the requirements set by Camerfirma, always subject to the applicable laws and regulations in force.

The Subordinate CAs that issue certificates under this hierarchy may be owned by Camerfirma or by other TSP. All the CAs that operate under this hierarchy do so from infrastructures technically controlled by Camerfirma.

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

- **INFOCERT-CAMERFIRMA CERTIFICATES 2024**

CN: INFOCERT-CAMERFIRMA CERTIFICATES 2024

Valid from (UTC time): 22/01/2023 11:55:18

Valid until (UTC time): 22/01/2045 11:55:18

Serial Number: 2E01 DAE2 81C0 16C3 14B3 EEC3 850A F1D8 14FA C663

X509v3 Subject Key Identifier: 16A8 FFF5 1905 E947 AAD2 561C 1008 F04D F69A 7359

Hash SHA-1: 2E92 F393 1E82 FF9D C65F 4341 6797 A8E2 6ABC 36DA

Hash SHA-256: E399 302E 4814 4670 6F9D 9218 BF76 E341 5989 9354 3592 418F 8638 CC08 2CAF E5DC

- **INFOCERT-CAMERFIRMA TIMESTAMP 2024**

CN: INFOCERT-CAMERFIRMA TIMESTAMP 2024

Valid from (UTC time): 22/01/2023 12:22:31

Valid until (UTC time): 22/01/2045 12:22:31

Serial Number: 40D6 A935 6F81 0EF7 050F 9C94 9EB3 7A83 8849 012A

X509v3 Subject Key Identifier: EF53 C938 3002 1F46 0A76 121C EBD3 7820 4097 7D81

Hash SHA-1: 75C4 C136 B314 3255 3C9C 0753 06DE ECB5 DDCB 6457

Hash SHA-256: 30C7 ABA8 8D1B 2915 BF3A 9AC9 32EB FB8E 61D0 E59D 9592 5569 40E0 ODA2 06F3 B85C

The following table shows the scheme of active Root CA and Subordinate CAs under this hierarchy, including, where applicable, the respective OIDs in the *Certificate Policies* extension of the certificates of each CA and of the different types of active certificates issued by each Subordinate CA under this CPS.

<u>INFOCERT-CAMERFIRMA CERTIFICATES 2024</u>	
INFOCERT-CAMERFIRMA QUALIFIED CERTIFICATES – 2024	
2.5.29.32.0 [anyPolicy]	
1.3.6.1.4.1.17326.10.21.1.1.2 [Camerfirma]	Qualified Citizen Certificate – Non-QSCD
0.4.0.194112.1.0 [ETSI EN 319 411-2 – QCP-n]	
INFOCERT-CAMERFIRMA TIMESTAMP 2024	
INFOCERT-CAMERFIRMA QUALIFIED TSA-2024	
2.5.29.32.0 [anyPolicy]	
1.3.6.1.4.1.17326.10.21.30.4 [Camerfirma]	Certificado Cualificado de TSU - QSCD HSM
0.4.0.194112.1.3 [ETSI EN 319 411-2 - QCP-l-qscd]	

* Each of the CAs aforementioned issues its corresponding OCSP certificate.

The following sections describe the Subordinate CAs under this CPS within the INFOCERT-CAMERFIRMA ROOT 2024 hierarchy, and, where applicable, the corresponding CPs for active issued certificates, except the CP of OCSP certificates (see section 1.3.1.5).

1.3.1.4.1 INFOCERT-CAMERFIRMA QUALIFIED CERTIFICATES - 2024

This Subordinate CA may issue qualified certificates to natural persons and legal persons (at present, only to natural persons) within the EU, in accordance with the requirements of eIDAS Regulation and Law 6/2020.

The identification details for this Subordinate CA certificate (issued by the Root CA of the INFOCERT-CAMERFIRMA ROOT 2024 hierarchy) are:

CN: INFOCERT-CAMERFIRMA QUALIFIED CERTIFICATES - 2024

Valid from (UTC time): 16/02/2024 12:55:23

Valid until (UTC time): 16/02/2040 12:55:23

Serial Number: 3DF7 30E0 DC99 52D7 BFF2 CD30 23D3 745F B203 1452

X509v3 Subject Key Identifier: A9D8 FB35 5AA4 AA49 2F72 3C55 0069 8024 2FCE 20CF

Hash SHA-1: 4C6D 9EFB 188E 7F02 4CD8 776A 743C 551A 1651 FCAD

Hash SHA-256: 8DOB 0805 D9B6 90BD 6E68 459B 56B1 20BE FE88 D6C3 35C5 F229 CA88 6E91 EC90 BBE5

The CPs of the active certificates issued by this Subordinate CA, except the PC of OCSP certificates (see section 1.3.1.5), are:

1.3.1.4.1.1 QUALIFIED CITIZEN CERTIFICATE

This qualified certificate identifies a natural person (Subject/Signatory) only to act on his/her own behalf (with no attributes).

1.3.1.4.2 INFOCERT-CAMERFIRMA QUALIFIED TSA - 2024

These Subordinate CAs issue certificates to legal persons for digital signing of time-stamps.

The identification details for this Subordinate CA certificate (issued by the Root CA of the INFOCERT-CAMERFIRMA ROOT 2024 hierarchy) are:

CN: INFOCERT-CAMERFIRMA QUALIFIED TSA - 2024

Valid from (UTC time): 16/02/2024 13:03:17

Valid until (UTC time): 16/02/2024 13:03:17

Serial Number: 28A4 A018 B3A1 2E20 5AF8 7934 98DE 7A3D 7B21 4C2B

X509v3 Subject Key Identifier: 8D94 321B 4155 0454 423A 2171 E911 9DF5 3480 AB5E

Hash SHA-1: 01BB 36A3 165A 4840 F635 E03B 41FD 11E6 D97E DEB8

Hash SHA-256: F1D4 8530 E034 940B 6553 37A1 B30B 0270 62B4 BA6D 6366 6DAB 1F99 3884 5267 23B3

The CPs of the active certificates issued by this Subordinate CA, except the PC of OCSP certificates (see section 1.3.1.5), are:

1.3.1.4.2.1 TSU QUALIFIED CERTIFICATE

This qualified certificate identifies a legal person (Subject / Creator of a Seal).

The Applicant for this certificate must have powers of representation that enable him/her to apply

for the certificate on behalf of the legal person to which the certificate is issued.

This certificate can be used for digital signing of time-stamps.

The keys of this certificate are generated and stored in an HSM QSCD, in accordance with the requirements set out in ETSI EN 319 421.

1.3.1.5 OCSP CERTIFICATES

Every Root CA and every Subordinate CA managed by Camerfirma within the hierarchies under this CPS issues an OCSP certificate, under the corresponding CP Non-Qualified OCSP Certificate, that will be used to sign the responses of the CA's OCSP service on the status of certificates issued by the CA, as long as the CA is active.

Additionally, the Subordinate CA AC CAMERFIRMA FOR NATURAL PERSONS (see section 1.3.1.1.1) issues *default* OCSP certificates, under the corresponding CP Non-Qualified OCSP Certificate, that will be used to sign the responses of the OCSP services of the CAs managed by Camerfirma within the hierarchies under this CPS, on:

- Status *unknown* of certificates issued by:
 - A CA outside the hierarchies under this CPS.
 - A CA that is not managed by Camerfirma within the hierarchies under this CPS.
 - A CA that is managed by Camerfirma within the hierarchies under this CPS and is terminated for a reason other than the compromise of its private key (see section 5.8.2).
- Corresponding status of certificates issued by:
 - A CA that is managed by Camerfirma within the hierarchies under this CPS and is terminated for compromise of its private key (see sections 5.7.3 and 5.8.2)

In the event of termination of the Subordinate CA issuing the *default* OCSP certificates, these will be replaced by *default* OCSP certificates issued, under the corresponding CP Non-Qualified OCSP Certificate, by another Camerfirma Subordinate CA within the same hierarchy.

In the event of termination of the Root CA of the hierarchy of the *default* OCSP certificates, these will be replaced by *default* OCSP certificate issued, under the corresponding CP Non-Qualified OCSP Certificate, by another Camerfirma Subordinate CA within another hierarchy under this CPS.

In the event of cessation of Camerfirma's activity as a TSP (see section 5.8.1), the OCSP services of all CAs managed by Camerfirma within the hierarchies under this CPS will no longer be available at their access addresses.

The keys of OCSP certificates issued, under the CPs Non-Qualified OCSP Certificate, by the CAs managed by Camerfirma within the hierarchies under this CPS are generated and stored in an HSM FIPS 140-2 level 3 or CC EAL 4 or higher, Non-QSCD or QSCD, in accordance with the requirements set out in ETSI EN 319 411-1.

1.3.1.6 TEST CERTIFICATES

The Subordinate CAs under this CPS may issue certificates with fictitious data to provide them to regulatory entities, as well as to application developers to be used in the integration or evaluation process for certificate acceptance. Camerfirma includes the following information in the certificates so that the Relying Party can see that it is a test certificate without liability:

Name of the Entity: **[SOLO PRUEBAS] ENTIDAD**
Tax ID No. of the Entity: **R0599999J**
Name of the natural person: **JUAN ANTONIO**
First surname of the natural person: **CÁMARA**
Second surname of the natural person: **ESPAÑOL**
National ID No. of the natural person: **00000000T**
CN: **[SOLO PRUEBAS] ...**

where '[SOLO PRUEBAS]' means '[TEST ONLY]'.

When a process requires the issuance of a test certificate with real data, this is done only after signing a confidentiality agreement with the entity responsible for the process. In this case, the data are specific to each customer, but '[SOLO PRUEBAS]' always appears before them in the name of the Entity and in the CN to identify at first glance that it is a test certificate without liability.

1.3.1.7 INTERNAL MANAGEMENT CA

Camerfirma has developed an internal management CA, named CAMERFIRMA GESTIÓN INTERNA, to issue RA operator certificates. With these certificates, operators can perform the actions related to their role on the certificate management platform.

The CA CAMERFIRMA GESTIÓN INTERNA is out of scope of these CPS and CPs.

1.3.2 REGISTRATION AUTHORITIES (RAS)

An RA may be a legal person or a natural person acting in accordance with this CPS and, if applicable, by means of an agreement with a Subordinate CA under this CPS (owned by Camerfirma), performing the functions of managing requests, identification and registration of end entity certificate Applicants, and, where applicable, processing requests for revocation and reports of events relating to revocation of end entity certificates, and any other responsibilities established in this document for the applicable CPs.

RAs are authorities delegated by Subordinates CAs, although the latter are ultimately responsible for the service.

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

- Chambers RA: 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.

- Remote RA: Corporate RA using third-party applications located in a remote location that communicates, through integration with a web services layer, with the certificate management platforms.

Under this CPS, the following can act as RA of Subordinate CAs:

- The CA (Camerfirma).
- The Spanish Chambers of Commerce, Industry, and Navigation, or the entities appointed by them.

They are obliged to pass the audits required in the contract with the CA.

- Spanish companies, as entities delegated by the CA or by another RA, to which they are contractually associated, to make the complete identification and registration of Applicant and, where applicable, processing requests for revocation and reports of events relating to revocation, within a particular organization or demarcation.

The operators of these RAs only manage requests and certificates in the scope of their organization or demarcation, unless determined otherwise by the CA or the RA on which they depend, for example, a corporation's employees, members of a corporate group and members of a professional body.

They are obliged to pass the audits required in the contract with the CA.

- Entities belonging to the Spanish Public Administrations.

They are obliged to pass the audits required in the contract with the CA.

- Other Spanish or international legal persons or agents that have a contractual relationship with the CA.

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.

They are obliged to pass the audits required in the contract with the CA.

- PPV. Point of Physical Verification that always depends on an RA. It may be a legal person or a natural person to whom the RA partially delegates the identification tasks.

Its main mission is to identify the Applicant by physical presence and deliver the documentation concerning the identification to the RA. For these functions, the PPVs are not subject to training or controls.

Sometimes, the PPVs' functions may be extended to collecting and collating the documentation submitted by the Applicant, checking its suitability for the type of certificate requested and delivering this documentation to the RA on which it depends, but a PVP can never validate the registration process and decide the certificate issuance.

An RA operator checks, in accordance with the applicable CP, the documentation provided by the PVP and, if applicable, the documentation submitted directly to the RA, and, if it is correct, proceeds with the issuance of the certificate by the CA, without having to make a

new identification of the Applicant.

Given that a PPV cannot register, it is contractually bound to an RA through a contract. Camerfirma has drafted a relationship model document between the RA and the PPV where the functions delegated by the RA to the PPV are defined.

- PRV. Point of Remote Verification that always depends on an RA. It may be a legal person or a natural person to whom the RA partially delegates the identification tasks.

Its main mission is to identify the Applicant using remote identification processes by video, which may be used to issue qualified certificates, as long as they comply with the conditions and technical requirements required by the applicable regulation. For these functions, the PRVs are subject to specific training and controls.

Sometimes, the PRVs' functions may be extended to receiving and collating the documentation submitted by the Applicant, checking its suitability for the type of certificate requested and delivering this documentation to the RA on which it depends, but a PRV can never validate the registration process and decide the certificate issuance.

After receiving the evidence of identification provided by the PRV, an RA operator checks, in accordance with the applicable CP, the documentation provided by the PRV and/or, if applicable, the documentation submitted directly to the RA, and, if it is correct, proceeds with the issuance of the certificate by the CA, without having to make a new identification of the Applicant.

Given that a PRV cannot register, it is contractually bound to an RA through a contract. Camerfirma has drafted a relationship model document between the RA and the PRV where the functions delegated by the RA to the PRV are defined.

1.3.3 SUBSCRIBERS

1.3.3.1 SUBSCRIBER

Under this CPS, and according to ETSI EN 319 401 standard, the Subscriber (with initial in capital letter) is the natural or legal person or the non-legal entity bound by agreement with Camerfirma, acting as a TSP issuing certificates (CAs under this CPS), and/or with an RA under this CPS to any Subscriber obligation for one or more certificates.

The Subscriber is the party that contracts Camerfirma (CAs under this CPS) and/or an RA under this CPS for the services of issuing one or more certificates. Therefore, the Subscriber of a certificate can be considered its owner.

Under these CPs, the Subscriber of a certificate can be:

- For certificates issued to natural persons without attributes of association with an Entity:
 - The natural person Subject.
 - A legal person or a non-legal entity with which the natural person Subject is

associated.

- For certificates issued to natural persons with attributes of association with an Entity (legal person or non-legal entity):
 - The natural person Subject.
 - The Entity (legal person or non-legal entity) identified in the certificate with which the natural person is associated.
 - A legal person or a non-legal entity with which the natural person Subject is associated (other than, where applicable, the Entity identified in the certificate).
- For certificates issued to legal persons
 - The Entity (legal person) Subject.
 - The Entity (legal person) identified in the certificate with which the Subject is associated, in the cases where the Subject is not the Entity.
 - A legal person with powers of representation of the Entity (legal person) Subject.
 - A legal person with powers of representation of the Entity (legal person) identified in the certificate with which the Subject is associated, in the cases where the Subject is not the Entity.

To avoid any conflict of interests, the Subscriber of a certificate and Camerfirma, as the TSP issuing the certificate (CAs under this CPS), or the RAs under this CPS shall be separate entities. The only exceptions are:

- A third party organization acting as an RA under this CPS and the Subscriber of the certificates issued for Subjects associated with it.
- Certificates that Camerfirma issues for itself (as a legal person) or natural persons belonging to it (as a Subject).

For both exceptions, the application, validation and processing of the certificates must be performed according to the processes defined by Camerfirma for the respective certificate types.

1.3.3.2 SUBJECT, SIGNATORY AND CREATOR OF A SEAL

Under this CPS, and according to ETSI EN 319 411-1 standard, the Subject (with initial in capital letter; also known as Holder) is the entity identified in a certificate (in its *Subject* field and, where applicable, in its *Subject Alternative Name* extension) as the holder of the private key associated with the public key contained in the certificate.

Under these CPs, the Subject of a certificate can be:

- For certificates issued to natural persons without attributes of association with an Entity:
 - The natural person to whom the certificate is issued. The Subscriber can be:
 - The Subject (the natural person identified in the certificate).

- A legal person or a non-legal entity with which the Subject is associated.
- For certificates issued to natural persons with attributes of association with an Entity (legal person or non-legal entity):
 - The natural person to whom the certificate is issued. The Subscriber can be:
 - The Subject (the natural person identified in the certificate).
 - The Entity identified in the certificate with which the natural person is associated (the legal person or the non-legal entity identified in the certificate).
 - A legal person or a non-legal entity with which the Subject is associated (other than, where applicable, the Entity identified in the certificate).
- For certificates issued to legal persons:
 - The Entity (legal person) to which the certificate is issued. The Subscriber is the Entity Subject (the legal person identified in the certificate) or another legal person with powers of representation of the Entity Subject.
 - An organization, unit, area or department associated with the Entity (legal person) to which the certificate is issued. The Subscriber is the Entity identified in the certificate with which the Subject is associated (the legal person identified in the certificate) or another legal person with powers of representation of the Entity identified in the certificate with which the Subject is associated.
 - A device, application or system operated by or on behalf of the Entity (legal person) to which the certificate is issued. The Subscriber is the Entity identified in the certificate with which the Subject is associated (the legal person identified in the certificate) or another legal person with powers of representation of the Entity identified in the certificate with which the Subject is associated.

Under this CPS, and according to eIDAS Regulation, the Signatory (with initial in capital letter) is the natural person identified in a certificate for electronic signature.

Under this CPS, and according to eIDAS Regulation, the Creator of a Seal (with initials in capital letters) is the legal person identified in a certificate for electronic seal.

Under these CPs, the Signatory and the Creator of a Seal of a certificate can be:

- For certificates issued to natural persons, with or without attributes of association with an Entity, qualified certificates, or non-qualified certificates with allowed use of signature:
 - The Signatory is the natural person Subject (the natural person identified in the certificate).
 - There is no Creator of a Seal.
- For all other certificates issued to natural persons (non-qualified certificates, with attributes of association with an Entity, without allowed use of signature):
 - There is no Signatory.

- There is no Creator of a Seal.
- For certificates issued to legal persons:
 - There is no Signatory.
 - The Creator of a Seal is the legal person identified in the certificate, which can be:
 - If the Subject is the Entity (legal person) to which the certificate is issued, the Creator of a Seal is the Entity (legal person), the Subject and, where applicable, the Subscriber.
 - If the Subject is an organization, unit, area or department associated with the Entity (legal person) to which the certificate is issued, the Creator of a Seal is the Entity (legal person) with which the Subject is associated and, where applicable, the Subscriber.
 - If the Subject is a device, application or system operated by or on behalf of the Entity (legal person) to which the certificate is issued, the Creator of a Seal is the Entity (legal person) with which the Subject is associated and, where applicable, the Subscriber.

The Signatory, as the natural person Subject of the certificate for electronic signature, shall be directly responsible for the obligations associated with the use and management of the certificate and its associated private key.

The Creator of a Seal, as the legal person Subject of the certificate for electronic seal, or as the legal person with which the Subject of the electronic seal certificate is associated, shall be directly responsible for the obligations associated with the use and management of the certificate and its associated private key, without prejudice to the obligations of the Person Responsible and, where applicable, of the Subject.

In these CPS and CPs, the term "Subject/Signatory" refers, in a generic way, to the Subject and/or Signatory of certificates issued to natural persons, and the term "Subject / Creator of a Seal" refers, in a generic way, to the Subject and/or Creator of a Seal of certificates issued to legal persons.

1.3.3.3 APPLICANT

Under this CPS, the Applicant (with initial in capital letter) is the natural person who requests a certificate for him/herself or for the legal entity which he/she represents.

During the certificate issuance process, the Applicant must be identified in accordance with section 3.2.3.

Under these CPs, the Applicant of a certificate can be:

- For certificates issued to natural persons, with or without attributes of association with an Entity:
 - The natural person Subject.
- For certificates issued to legal persons:

- A natural person with powers of representation that enable him/her to apply for the certificate on behalf of the Entity (legal person) to which the certificate is issued.

1.3.3.4 PERSON RESPONSIBLE

Under this CPS, the Person Responsible (with initials in capital letters) is the natural person responsible for the use of the private key associated with the public key contained in a certificate.

During the certificate issuance process, the Person Responsible performs, among the following functions, those applicable to the type of device where the certificate keys are generated: deliver the public key, receive the private key, define and/or receive the private key activation data, receive the certificate.

Under these CPs, the Applicant of a certificate can be:

- For certificates issued to natural persons, with or without attributes of association with an Entity:
 - The natural person Subject and Applicant.
- For certificates issued to legal persons:
 - The Applicant, or a natural person authorized by the Applicant, without prejudice to the obligations of the Creator of a Seal and, if applicable, the Subject.

1.3.3.5 ENTITY

Under this CPS, the Entity (with initial in capital letter) is, where applicable, the public or private, individual or collective organization, recognized in law, as identified in the *organizationName* (O) and *organizationIdentifier* attributes of *subject* field of a certificate, with which the Subject has a certain association, or which identifies the Subject.

Under these CPs, the Entity of a certificate can be:

- For certificates issued to natural persons without attributes of association with an Entity:
 - There is no Entity.
- For certificates issued to natural persons with attributes of association with an Entity (legal person or non-legal entity):
 - The Entity with which the natural person is associated (the legal person or the non-legal entity identified in the certificate).
- For certificates issued to legal persons, the legal person identified in the certificate, which can be:
 - If the Subject is the Entity (legal person) to which the certificate is issued, the Subject, Subscriber and Creator of a Seal.
 - If the Subject is an organization, unit, area or department associated with the Entity

- (legal person) to which the certificate is issued, the Subscriber and Creator of a Seal.
- If the Subject is a device, application or system operated by or on behalf of the Entity (legal person) to which the certificate is issued, the Subscriber and Creator of a Seal.

1.3.4 RELYING PARTIES

In these CPS and CPS, the Relaying Party is the person or organization that voluntarily relies on a certificate issued by any of the CAs under this CPS.

1.3.5 OTHER PARTICIPANTS

1.3.5.1 SUPERVISORY BODY

The Supervisory Body (also known as Accreditation Body) is the corresponding management body that accepts, accredits, and supervises the Trust Service Providers (TSPs) within a specific geographic area.

The national Supervisory Body within the Spanish State is currently the *Ministerio de Asuntos Económicos y Transformación Digital*, which is the competent authority appointed for these tasks by the Spanish Member State of the European Economic Space.

External Subordinate CAs may be subject to legal frameworks in different countries or regions. In such cases, the accreditation of the Entity falls on the corresponding national bodies.

1.3.5.2 TRUST SERVICE PROVIDER (TSP) AND QUALIFIED TRUST SERVICE PROVIDER (QTSP)

According to eIDAS Regulation, a Trust Service Provider (TSP) is a natural person or legal person who provides one or more trust services either as a Qualified or as a Non-Qualified Trust Service Provider.

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

According to ETSI EN 319 401 standard a Trust Service Provider (TSP) is an entity which provides one or more trust services.

The trust services defined in the eIDAS Regulation include:

- Creation, verification, and validation of electronic signatures and certificates related to those services.
- Creation, verification, and validation of electronic seals and certificates related to those services.

- Creation, verification, and validation of electronic time stamps and certificates related to those services.
- Electronic registered delivery services and certificates related to those services.
- Creation, verification, and validation of certificates for website authentication.
- Preservation of electronic signatures and certificates related to those services.
- Preservation of electronic seals and certificates related to those services.

The trust services defined in ETSI EN 319 401 standard include:

- Creation, verification and validation of digital signatures and related certificates.
- Creation, verification and validation of time-stamps and related certificates.
- Registered delivery and related certificates.
- Creation, verification and validation of certificates for website authentication; or
- Preservation of digital signatures or certificates related to those services.

Under these CPS and CPs, the terms TSP and QTSP refer to Camerfirma, acting as the certificate issuer TSP (CA), and to other TSPs and QTSPs.

1.4 CERTIFICATE USAGE

1.4.1 APPROPRIATE CERTIFICATE USES

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

- Subject authentication.
- Advanced electronic signature, or qualified electronic signature when used with qualified electronic signature creation devices.
- Advanced electronic seal, or qualified electronic seal when used with qualified electronic seals creation devices.
- Asymmetric or mixed encryption without key recovery.

1.4.2 PROHIBITED CERTIFICATE USES

Camerfirma includes information on the limitation of use in the certificate, either in the standard extensions *Key Usage* and *Basic Constraints* marked as "critical" in the certificate, and therefore mandatory for the applications that use it, or limitations in standard extensions such as *Extended Key Usage* and *Name Constraints* and/or through texts included in the field *User Notice* in the standard extension Certificate Policies, marked as "non-critical", but mandatory for the Subject

and Relying Parties.

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

The certificates are not designed, may not be used and 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 certificates in transactions that contravene the CP applicable to each of the certificates, the CPS, the Terms and Conditions or the contracts that the CAs sign with the RAs or with the Subscribers is considered illegal, and the CA is exempt from any liability due to the Subjects or third party's misuse of the certificates in accordance with current law.

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

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

1.5 POLICY ADMINISTRATION

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

1.5.1 ORGANIZATION ADMINISTERING THE DOCUMENT

The drafting and revision of this document are done by the Camerfirma compliance and legal departments in collaboration with the Operation and System departments.

1.5.2 CONTACT PERSON

Address: Calle de Rodríguez Marín 88 – 28016 Madrid (Spain)

Telephone: +34 91 136 91 05

Email: info@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 active certificates issued under this CPS, you can contact Camerfirma by sending an email to the address 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://www.camerfirma.com/practicas-de-certificacion-ac-camerfirma-cps-dpc/>. The CPS is published in PDF format electronically signed or sealed with the digital certificate of the approver.

1.6 DEFINITIONS AND ACRONYMS

1.6.1 DEFINITIONS

Activation data	Private data such as PINs or passwords used to activate the private key.
Advanced electronic seal	Electronic seal, which meets the requirements set out in Article 36: <ul style="list-style-type: none"> a) it is uniquely linked to the Creator of the Seal; b) it is capable of identifying the Creator of the Seal; c) it is created using electronic seal creation data that the Creator of the Seal can, with a high level of confidence under its control, use for electronic seal creation; and d) it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable.
Advanced electronic	Electronic signature which meets the requirements set out in Article 26 of

signature	eIDAS Regulation: a) it is uniquely linked to the Signatory; b) it is capable of identifying the Signatory; c) it is created using electronic signature creation data that the Signatory can, with a high level of confidence, use under his sole control; and d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.
Applicant	Natural person who requests a certificate for him/herself or for the legal entity which he/she represents.
CA Certificate	Certificate issued to a CA by another CA or by the same CA, whose private key is used for signing certificates and/or CRLs.
Certificate	A file that associates the public key with some data of the Subject and is signed by the CA.
Certificate for electronic seal	Electronic attestation that links electronic seal validation data to a legal person and confirms the name of that person.
Certificate for electronic signature	Electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person.
Certificate Policy	Set of rules defining the applicability of a certificate to a community and/or a set of applications or uses with common security and usage requirements.
Certification Authority	Entity responsible for issuing and managing certificates. It acts as the trusted third party between the Subject and the Relying Party, associating a specific public key with the Subject. Trust Service Provider that issues certificates.
Certification Practice Statement	Set of practices adopted by a Certification Authority for the issuance, management, revocation, and renewal or re-key of certificates.
Creator of a Seal	Legal person identified in a certificate for electronic seal. Person who creates an electronic seal.
CRL	File containing a list of certificates that have been revoked at a certain date and time and which is signed by the CA.
Cross certification	Establishment of a trust relationship between two CAs, by the issuance of a certificate by one CA to the other CA.
Digital signature	Result of the transformation of a message, or any type of data, by the private key application in conjunction with known algorithms, thus ensuring:

	<p>a) that the data has not been modified (integrity);</p> <p>b) that the person signing the data is who he/she claims (identification); and</p> <p>c) that the person signing the data cannot deny having done so (non-repudiation at origin).</p>
Electronic seal	Data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity.
Electronic seal creation data	Unique data, which is used by the Creator of the electronic Seal to create an electronic seal. Also called private key.
Electronic seal creation device	Configured software or hardware used to create an electronic seal.
Electronic signature	Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the Signatory to sign.
Electronic signature creation data	Unique data which is used by the Signatory to create an electronic signature. Also called private key.
Electronic signature creation device	Configured software or hardware used to create an electronic signature.
Electronic time stamp	Data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time.
End entity	Subject of a certificate issued by a CA, whose private key is not used for signing certificates and/or CRLs.
End entity certificate	Certificate issued to an end entity by a CA, whose private key is not used for signing certificates and/or CRLs.
Entity	Public or private, individual or collective organization, recognized in law, as identified in the <i>organizationName</i> (O) and <i>organizationIdentifier</i> attributes of <i>Subject</i> field of a certificate, with which the Subject has a certain association, or which identifies the Subject.
Hash	Operation performed on a set of data of any size, so that the result obtained is another set of data of fixed size, regardless of the original size, and which has the property of being univocally associated with the initial data.
HSM	Hardware device that generates and protects cryptographic keys, and allows using them to perform cryptographic operations in a secure way.
Key pair	Set consisting of a public and private key, both related to each other mathematically.

OID	Unique numeric identifier registered under the ISO standardization and referring to a particular object or object class.
Person Responsible	Natural person responsible for the use of the private key associated with the public key contained in a certificate.
PKI	Set of hardware, software, human resources , procedures, etc., that make up a system used for the creation and management of public key certificates.
Policy Authority	Person or group of people responsible for all decisions relating to the creation, management, maintenance, and removal of CPs and CPSs.
Private key	Mathematical value used only by the Subject for creating a digital signature or decrypting data. Also called electronic signature creation data and electronic seal creation data.
Public key	Publicly known mathematical value used for verifying a digital signature or encrypting data. Also called validation data.
Qualified certificate for electronic seal	Certificate for electronic seal, that is issued by a Qualified Trust Service Provider and meets the requirements laid down in Annex III of eIDAS Regulation.
Qualified certificate for electronic signature	Certificate for electronic signature, that is issued by a Qualified Trust Service Provider and meets the requirements laid down in Annex I of eIDAS Regulation.
Qualified electronic seal	Advanced electronic seal, which is created by a Qualified electronic Seal Creation Device, and that is based on a qualified certificate for electronic seal.
Qualified electronic Seal Creation Device	Seal creation device that meets <i>mutatis mutandis</i> the requirements laid down in Annex II of eIDAS Regulation.
Qualified electronic signature	Advanced electronic signature that is created by a Qualified electronic Signature Creation Device, and which is based on a qualified certificate for electronic signatures.
Qualified electronic Signature Creation Device	Signature creation device that meets the requirements laid down in Annex II of eIDAS Regulation.
Qualified electronic time stamp	Electronic time stamp which meets the requirements laid down in Article 42 of eIDAS Regulation: a) it binds the date and time to data in such a manner as to reasonably

	<p>preclude the possibility of the data being changed undetectably;</p> <p>b) it is based on an accurate time source linked to Coordinated Universal Time; and</p> <p>c) it is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by some equivalent method.</p>
Qualified Trust Service Provider	Trust Service Provider who provides one or more qualified trust services and is granted the qualified status by the Supervisory Body
Registration Authority	Entity responsible for managing requests, identification and registration of end entity certificate Applicants, and, where applicable, for processing requests for revocation and reports of events relating to revocation of end entity certificates.
Relying Party	Person or organization that voluntarily relies on a certificate issued by any of the CAs under this CPS.
Remote Seal	Special procedure of electronic seal generated by an HSM that guarantees the control of the private key by the Creator of a Seal and that allows the creation of electronic seals remotely.
Remote Signature	Special procedure of electronic signature generated by an HSM that guarantees the sole control of the private key by the Signatory and allows the creation of electronic signatures remotely.
Secure cryptographic device	Device which holds the user's private key, protects this key against compromise and performs signing and/or decryption functions on behalf of the user.
Signatory	Natural person identified in a certificate for electronic signature. Natural person who creates an electronic signature
Subject	Entity identified in a certificate as the holder of the private key associated with the public key contained in the certificate. Also called Holder.
Subscriber	Natural or legal person or the non-legal entity bound by agreement with Camerfirma, acting as a Trust Service Provider issuing certificates (Certification Authorities), to any Subscriber obligation for one or more certificates.
Supervisory Body	Corresponding management body that accepts, accredits, and supervises the Trust Service Providers within a specific geographic area. Also called Accreditation Body. The national Supervisory Body within the Spanish State is currently the <i>Ministerio de Asuntos Económicos y Transformación Digital</i> .
Trust service	Electronic service normally provided for remuneration which consists of:

	<p>a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or</p> <p>b) the creation, verification and validation of certificates for website authentication; or</p> <p>c) the preservation of electronic signatures, seals or certificates related to those services.</p>
Trust Service Provider	Natural or a legal person who provides one or more trust services either as a Qualified or as a Non-Qualified Trust Service Provider
Time-Stamping Authority	Trust Service Provider providing time-stamping services using one or more Time-Stamping Units.
Time-Stamping Unit	Set of hardware and software which is managed as a unit and has a single time-stamp signing key active at a time.
Validation data	Data that is used to validate an electronic signature or an electronic seal. Also called public key.

1.6.2 ACRONYMS

AWS	Amazon Web Services
CA	Certification Authority
CAA	Certification Authority Authorization
CC	Common Criteria
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DN	Distinguished Name.
DNI	<i>Documento Nacional de Identidad</i> . National Identity Document.
EAL	Evaluation Assurance Level
EEA	European Economic Area
eIDAS	electronic IDentification, Authentication and trust Services
EN	European Standard

ETSI	European Telecommunications Standards Institute
EU	European Union
FIPS	Federal Information Processing Standard
GDPR	General Data Protection Regulation
GPS	Global Positioning System
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO	International Organization for Standardization
ITU	International Telecommunication Union
LOPDGDD	<i>Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales</i> . Spanish Organic Law on the Protection of Personal Data and Guarantee of Digital Rights.
NCP	Normalized Certificate Policy
NCP+	Extended Normalized Certificate Policy
NIE	<i>Número de Identidad de Extranjero</i> . Foreigner Identity Number.
NIF	<i>Número de Identificación Fiscal</i> . Tax Identification Number.
NTP	Network Time Protocol
O	Organization name
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PA	Policy Authority
PDF	Portable Document Format
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
PPV	Point of Physical Verification
PRV	Point of Remote Verification

QCP-I	Certificate Policy for EU Qualified Certificates issued to legal persons
QCP-I-qscd	Certificate Policy for EU Qualified Certificates issued to legal persons where the private key and the related certificate reside on a QSCD
QCP-n	Certificate Policy for EU Qualified Certificates issued to natural persons
QCP-n-qscd	Certificate Policy for EU Qualified Certificates issued to natural persons where the private key and the related certificate reside on a QSCD
QSCD	Qualified electronic Signature/Seal Creation Device.
QTSP	Qualified Trust Service Provider
RA	Registration Authority
ROA	<i>Real Instituto y Observatorio de la Armada</i> . Spanish Royal Navy Institute and Observatory
RSA	Rivest-Shamir-Adleman (type of public key algorithm)
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer (secure communication protocol)
TLS	Transport Layer Security (secure communication protocol that replaces SSL)
TSA	Time-Stamping Authority
TSL	Trust-service Status List
TSP	Trust Service Provider
TSU	Time-Stamping Unit
UTC	Coordinated Universal Time

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

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

In the event of a system failure, or any other circumstance out of Camerfirma's control, Camerfirma shall apply best endeavours to ensure that these repositories are not unavailable for longer than 24 hours.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

2.2.1 CERTIFICATION PRACTICES AND CERTIFICATE POLICIES

Camerfirma makes available to the public the current version of these CPS and CPs on the website at the following addresses:

- <https://www.camerfirma.com/practicas-de-certificacion-ac-camerfirma-cps-dpc/>
- <https://policy.camerfirma.com>
- <https://policy2021.camerfirma.com>

When a new version of these CPS and CPs is published, Camerfirma will keep available to the public the previous version on the same website, at least until termination of all CAs included in that version (see section 5.8.2).

2.2.2 TERMS AND CONDITIONS

The Person Responsible, and the Subject and/or the Subscriber if they are different, receive information on the Terms and Conditions to be accepted before the issuance of the certificate.

Relying Parties can also consult the current version of the Terms and Conditions on the Camerfirma website:

<https://www.camerfirma.com/condiciones-de-uso-certificados-ac-camerfirma/>

2.2.3 DISTRIBUTION OF THE CERTIFICATES

Camerfirma makes available to the public the certificates of the Root and Subordinate CAs owned by Camerfirma under this CPS, their corresponding OCSP certificates and their respective hashes SHA-1 and SHA-256 on the website:

<https://www.camerfirma.com/autoridades-de-certificacion/>

Camerfirma will continue to make available to the public the certificates of the terminated CAs (see section 5.8.2) and their respective hashes SHA-1 and SHA-256 on the same website, for at least 15 years after the expiry of all certificates issued by the CA or until the cessation of Camerfirma's activity as a TSP (see section 5.8.1).

In the event of cessation of Camerfirma's activity as a TSP, the provision of Camerfirma CAs' certificates shall be guaranteed by Camerfirma or by a reliable party to whom it transfers this obligation, for at least 15 years after the expiry of all certificates issued by the CAs.

The certificate of a CA can be accessed via the HTTP protocol at the access address contained in the extension *Authority Information Access* of certificates issued by the CA.

Camerfirma shall make end entity certificates issued by Subordinate CAs under this CPS available to their respective Subscribers, Subjects and Persons Responsible, and, where applicable, to other QTSPs or TSPs managing the private key on behalf of the Subjects in accordance with the specific procedure for issuing the type of certificate.

Camerfirma shall not make end entity certificates issued by Subordinate CAs under this CPS available to Relying Parties, except for OCSP certificates and TSU certificates owned by Camerfirma.

Camerfirma shall make available to the public TSU certificates owned by Camerfirma under this CPS and their corresponding issuer CAs on the website:

<https://www.camerfirma.com/servicios-y-soluciones/sellado-de-tiempo/>

Camerfirma shall make external Subordinate CAs certificates issued by Root and Subordinate CAs under this CPS available to their respective owning Entities, in accordance with the specific procedure for issuing the type of certificate.

Camerfirma shall only make external Subordinate CAs certificates issued by Root and Subordinate CAs under this CPS available to Relying Parties, if this has been agreed with their respective owning Entities.

2.2.4 CRL AND OCSP

Camerfirma makes available to the public the CRLs of the Root and Subordinate CAs owned by Camerfirma under this CPS and the access addresses of their corresponding OCSP servers on the website:

<https://www.camerfirma.com/autoridades-de-certificacion/>

Camerfirma will make available to the public the last CRLs of the terminated CAs (see section 5.8.2) and their respective hashes SHA-1 and SHA-256 on the same website, for at least 15 years after the expiry of all certificates issued by the CA or until the cessation of Camerfirma's activity as a TSP (see section 5.8.1).

In the event of cessation of Camerfirma's activity as a TSP, the provision of revocation status information on the certificates issued by Camerfirma's CAs shall be guaranteed by Camerfirma or by a reliable party to whom it transfers this obligation, through the CAs' last CRLs, for at least 15 years after the expiry of all certificates issued by the CAs.

The CRL/s of a CA can be accessed via the HTTP protocol at the access addresses contained in the extension *CRL Distribution Points* of certificates issued by the CA.

The OCSP service of a CA can be accessed via the HTTP protocol at the access address contained in the extension *Authority Information Access* of certificates issued by the CA.

In the event of cessation of Camerfirma's activity as a TSP, the OCSP services of all CAs under this CPS will no longer be available at their access addresses.

The primary certificate status service of CAs under this CPS is the one provided by their OCSP service.

2.3 TIME OR FREQUENCY OF PUBLICATION

A new version of these CPS and CPs will be created at least once a year. Camerfirma immediately publishes on its website any new version of these CPS and CPs.

CAs under this CPS issue and publish CRLs with the frequency and maximum latency specified in sections 4.9.7 and 4.9.8.

Camerfirma shall update the information provided via the OCSP service of each CA under this CPS with the frequency and maximum latency specified in section 4.9.10.

2.4 ACCESS CONTROLS TO REPOSITORIES

Access to Camerfirma repositories for publication of certification information is free of charge, except for:

- End entity certificates shall only be available to their respective Subscribers, Subjects and Persons Responsible, except for OCSP certificates and TSU certificates owned by Camerfirma.
- External Subordinate CAs certificates shall only be available to their respective owning Entities, unless these have agreed with Camerfirma to make them public.

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 TYPES OF NAMES

The Subject's data (names) is included in the *Subject* field of the certificate, by means of a Distinguished Name (DN) in accordance with the reference standard X.500 in ISO/IEC 9594 and, where applicable, in the fields of the *Subject Alternative Name* extension of the certificate.

The structure and content of the DN in the *Subject* field and, where applicable, in the fields of the *Subject Alternative Name* extension of the certificate are described in the certificate profiles datasheets, including at least:

- For end entity certificates issued to natural persons without attributes of association with an Entity:
 - Name and surname and tax identification number of the natural person Subject.
- For end entity certificates issued to natural persons with attributes of association with an Entity (legal person or non-legal entity):
 - Name and surname and tax identification number of the natural person Subject.
 - Full registered name and tax identification number of the Entity.

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

- For end entity certificates issued to legal persons, except for TSU and OCSP certificates:
 - If the Subject is the Entity (legal person) to which the certificate is issued:
 - Full registered name and tax identification number of the Entity.
 - If the Subject is an organization, unit, area or department associated with the Entity (legal person) to which the certificate is issued:
 - Full registered name and tax identification number of the Entity.
 - Name of the organization, unit, area or department.
 - If the Subject is a device, application or system operated by or on behalf of the Entity (legal person) to which the certificate is issued:
 - Full registered name and tax identification number of the Entity.
 - Name of the device, application or system.
- For CA, TSU and OCSP certificates (issued to legal persons), in the DN in the *Subject* field:
 - Descriptive name of the CA, the TSU or the OCSP service (CN).

- Full registered name of the owning legal person (*O*).
- Tax identification number of the owning legal person (*organizationIdentifier* and/or *serialNumber*)
- Country where the owning legal person carries out the activity (*C*).

Datasheets of certificate profiles under these CPS and CPs can be requested through Camerfirma customer support service on the website <https://www.camerfirma.com/contacto-soporte/> or by telephone +34 91 136 91 05

3.1.2 NEED FOR NAMES TO BE MEANINGFUL

All DN are meaningful, and the identification of the attributes associated with the Subject is in a human-readable form.

3.1.3 PSEUDONYMS

Camerfirma will use the pseudonym in certificates in which it is allowed in *CN* and *pseudonym* attributes of DN, keeping the Subject/Signatory's real identity confidential.

The pseudonym is calculated in such a way that the real Subject is unmistakably identified.

3.1.4 RULES USED TO INTERPRET SEVERAL NAME FORMATS

Camerfirma complies with the reference standard X.500 in ISO/IEC 9594, IETF RFC 5280 and RFC 3739 standards and the applicable ETSI EN 319 412 standards.

3.1.5 UNIQUENESS OF NAMES

Within a single CA, names of a Subject that have already been taken cannot be re-assigned to a different Subject. This is ensured by including the unique tax identification number of the Subject in the DN of the certificate.

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 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 in accordance with the order in which they are registered.

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: the keys are given to the Person Responsible in person or by email 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 QSCD SmartCard/Token: the keys can be delivered by Camerfirma to the Person Responsible, directly or through a RA on a device cryptographic smartcard/token QSCD, that complies with the requirements set out in Annex II of the eIDAS Regulation.

In SmartCard/Token (Non-QSCD or QSCD smartcard/token): the keys can be delivered by Camerfirma to the Person Responsible, directly or through a RA on a device cryptographic smartcard/token FIPS 140-2 level 3 or CC EAL 4 or higher, Non-QSCD or QSCD.

In QSCD Cloud (QSCD centralized platform): Camerfirma uses a remote key storage system, allowing the Subject to access the private key from different devices. The keys are stored in an HSM QSCD, which allows the Subject/Signatory (or the Subject / Creator of a Seal, in the case of a legal entity) to use the private key under his/her sole control (or under its control, in the case of a legal entity), and that complies with the requirements set out in Annex II of the eIDAS Regulation.

In Cloud (Non-QSCD or QSCD centralized platform): Camerfirma uses a remote key storage system, allowing the Subject to access the private key from different devices. The keys are stored in an HSM FIPS 140-2 level 3 or CC EAL 4 or higher, Non-QSCD or QSCD, which allows the Subject/Signatory (or the Subject / Creator of a Seal, in the case of a legal entity) to use the private key under his/her sole control (or under its control, in the case of a legal entity).

2) Keys created by the Subject

The Subject has a key generation mechanism, either software or hardware. These keys are generated in an external device that is not managed by Camerfirma or another QTSP or TSP, so Camerfirma cannot guarantee that the device is QSCD and is therefore classified as Non-QSCD,

except in the case of QSCD HSM (TSU certificate by means of a declaration of responsibility). 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 issuance of a certificate to a legal person or to a natural person with attributes of association with an Entity, it is necessary to verify the data relating to the constitution and, if applicable, the legal personality of the Entity.

For these certificates, the identification of the Entity is required in all cases, for which the RA, depending on each case, will require the relevant documentation according to the type of Entity and/or will perform queries at the registration agencies used for the identification of the Entities.

The relevant documentation according to the type of Entity can be found on the Camerfirma website, in the informative section of the corresponding certificate.

For Public Administrations, documentation accrediting the existence of the Public Administration, body, public body or public law entity is not required, because this identity is part of the institutional scope of the General State Administration or other Public Administrations of the State.

In 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.*
 - Specific registration agency according to Entity type.

Additionally, for those certificates in which the Subscriber is different from the Subject and, where applicable, from the Entity, the identification of the Subscriber (legal person or non-legal entity) is required in the same way as for the identification of the Entity.

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 under this CPS.

3.2.2.5 AUTHENTICATION OF AN IP ADDRESS

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

3.2.2.6 WILDCARD DOMAIN VALIDATION

No SSL/TLS certificates are being issued by the CAs under 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 under 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, where applicable, must 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 with NIE:
 - Passport or national identity document issued by UE or EEA country and *Certificado de Número de Identidad de Extranjero* (NIE).
- Foreigners from UE or EEA without NIE but with NIF:
 - Passport or national identity document issued by UE or EEA country.
- Foreigners from UE or EEA without NIE or NIF:

- Passport or national identity document issued by UE or EEA country.
- Foreigners from other countries residing in Spain (with NIE):
 - Residence Card or Foreigner Identity Card with photography.
- Foreigners from other countries not residing in Spain (without NIE) but with NIF:
 - Passport and *Certificado de Número de Identificación Fiscal* (NIF).

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

Identification methods:

The identity of the Applicant of a qualified certificate 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 CA operator, an RA Operator, or a PPV (Point of Physical Verification) operator. The Applicant may alternatively choose to come along a Public Notary and provide the certificate issuance request with his/her signature authenticated.
- 2) Remotely, using electronic identification means, for which prior to the issuance of the qualified certificate, a physical presence of the Applicant was ensured and which meets the requirements set out in Article 8 of eIDAS Regulation with regard to the assurance levels 'substantial' or 'high'. Electronic identification systems notified by the Member States under Article 9.1 of the eIDAS Regulation shall be accepted. In the case of Spain, the electronic DNI shall be accepted.
- 3) By means of a certificate of a qualified electronic signature issued by a Camerfirma CA or another QTSP CA, for which the Applicant has been identified in person by the issuer QTSP, either directly or by relying on a third party in accordance with national law, or using electronic identification means by point 2 above, provided that the Applicant's identity data are contained in the certificate used.

If the certificate used also contains the attributes of association of the Applicant with an Entity and the identity data of this Entity which will be contained in the certificate applied for, the provisions of section 3.2.2.1 on the verification of the data relating to the constitution and, if applicable, the legal personality of the Entity, and the provisions of section 3.2.5.1 on the submission of documentation for the verification of the association of the Applicant with the Entity, are not required.

- 4) Other identification methods recognized at 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 certificates, as long as they comply with the conditions and technical requirements required by the applicable regulation, which must be confirmed in the report issued by a conformity assessment body, specifically the following:

- Assisted process, with synchronous mediation of an operator.
- Unattended process, without online interaction with an operator, 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 shall check the Applicant's identity data, using the document number, through the Data Verification and Consultation Service that the Supervisory Body makes available, provided that the technical requirements of the platform and the DNI or NIE accreditation support allow it.
- Registration data, i.e. audio and video files and structured metadata in electronic format are stored in a protected manner and in accordance with the European standard on personal data protection.
- For security and fraud prevention purposes, only conventional identity documents will be accepted under this method of identification (Spanish ID cards and Spanish or foreign passports). The identification of foreign Applicants who do not have a passport may be authorized by the CA 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 of the Applicant for a qualified certificate, the provisions of section 3.2.2.1 on the verification of the data relating to the constitution and, if applicable, the legal personality of the Entity, and the provisions of section 3.2.5.1 on the submission of documentation for the verification of the association of the Applicant with the Entity may not be required when the identity or other permanent circumstances of the certificate Applicant are already known by Camerfirma or the RA by a pre-existing relationship, in which, for the identification of the Applicant, the means indicated in point 1) were used and the period that has elapsed since the identification is less than five years.

The identity of the Applicant of a non-qualified certificate shall be verified using one of the methods for verifying the identity of the Applicant of a qualified certificate indicated in this section, or any of the following alternative methods:

- 1) By means of a qualified certificate of an advanced electronic signature (qualified or non-qualified electronic signature) issued by a Camerfirma CA or another QTSP, or by means of a certificate of an advanced electronic signature issued by another CA trusted by the RA or the CA, with no requirements regarding the identification method used to issue it.

2) Remote video identification methods not recognized at national level.

3.2.4 NON-VERIFIED SUBSCRIBER INFORMATION

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

3.2.5 VALIDATION OF AUTHORITY

3.2.5.1 VERIFICATION OF ASSOCIATION OF THE APPLICANT AND THE PERSON RESPONSIBLE WITH THE ENTITY

Certificate type	Documentation
Qualified Corporate Certificate	Usually, authorization signed by an Entity's legal representative.
Qualified Corporate Certificate for a Self-employed Qualified Corporate Certificate for a Chartered Self-employed	Documentation accrediting the status of self-employed under the economic activity regime, and if he/she is a professional member of a professional association (subscription in force). Optionally, documentation accrediting the registered trade name under which the activity is carried out.
Qualified Certificate for a Representative of a Legal/Non-Legal Entity with general powers of representation Qualified Certificate for a Voluntary Representative of a Legal/Non-Legal Entity before the Public Administrations Qualified Certificate for a Special Representative of a Legal/Non-Legal Entity	Documentation accrediting Entity's representation powers, depending on the type of representative and on the type of entity.
Certificates for a Public Employee With/Without a Pseudonym	Authorization signed by a person with powers of representation of the Entity indicating that he/she is a public employee, or appointment in the Official State Gazette where this person's DNI/NIE No. appears.
Qualified Certificate for Electronic Seal	In case the Applicant and the Person Responsible are different persons,

	<p>authorization signed by the Applicant (authorizing person) to the Person Responsible (authorized person), to request and be given the certificate and make use of it.</p> <p>Certificate or consultation of the Companies Registry to verify constitution and legal personality of the Entity, and appointment and validity of the position of the Applicant (if applicable, at the same time, authorizing person) with powers of representation that allow him/her to apply for the certificate on behalf of the Entity (legal person).</p>
<p>Qualified Certificate for Electronic Seal for Public Administrations</p>	<p>In case the Applicant and the Person Responsible are different persons, authorization signed by the Applicant (authorizing person) to the Person Responsible (authorized person), to request and be given the certificate and make use of it.</p> <p>Certificate to verify appointment and validity of the position of the Applicant (if applicable, at the same time, authorizing person) with powers of representation that allow him/her to apply for the certificate on behalf of the Entity (legal person), or appointment in the Official State Gazette where this person's DNI/NIE No. appears.</p>
<p>TSU Qualified Certificate TSU Non-Qualified Certificate Code Signing Non-Qualified Certificate</p>	<p>In case the Applicant and the Person Responsible are different persons, authorization signed by the Applicant (authorizing person) to the Person Responsible (authorized person), to request and be given the certificate and make use of it.</p> <p>In case the Entity is not a Public Administration, certificate or consultation of the Companies Registry to verify constitution and legal personality of the Entity, and appointment and validity of the position of the Applicant (if applicable, at the same time, authorizing person) with powers of representation that allow him/her to apply for the certificate on behalf of the Entity (legal</p>

	<p>person).</p> <p>In case the Entity is a Public Administration, certificate to verify appointment and validity of the position of the Applicant (if applicable, at the same time, authorizing person) with powers of representation that allow him/her to apply for the certificate on behalf of the Entity (legal person), or appointment in the Official State Gazette where this person's DNI/NIE No. appears.</p>
Non-Qualified Certificate for Electronic Seal	<p>In case the Applicant and the Person Responsible are different persons, authorization signed by the Applicant (authorizing person) to the Person Responsible (authorized person), to request and be given the certificate and make use of it.</p> <p>Certificate or consultation of the Companies Registry to verify constitution and legal personality of the Entity, and appointment and validity of the position of the Applicant (if applicable, at the same time, authorizing person) with powers of representation that allow him/her to apply for the certificate on behalf of the Entity (legal person).</p>
Non-Qualified Certificate for Electronic Seal for Public Administrations	<p>In case the Applicant and the Person Responsible are different persons, authorization signed by the Applicant (authorizing person) to the Person Responsible (authorized person), to request and be given the certificate and make use of it.</p> <p>Certificate to verify appointment and validity of the position of the Applicant (if applicable, at the same time, authorizing person) with powers of representation that allow him/her to apply for the certificate on behalf of the Entity (legal person), or appointment in the Official State Gazette where this person's DNI/NIE No. appears.</p>
Non-Qualified Certificate for Personnel for Public Administrations	<p>Authorization signed by a person with powers of representation of the Entity indicating that he/she is a public employee, or appointment in</p>

the Official State Gazette where this person's DNI/NIE No. appears.

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 for preservation in computer files.

3.2.5.2 SERVICE OR MACHINE IDENTITY

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

3.2.5.3 SPECIAL CONSIDERATIONS FOR ISSUING CERTIFICATES OUTSIDE OF SPANISH TERRITORY

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.

3.2.6 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 of a certificate is the process that must be carried out to obtain a new key pair and a new certificate before its expiry date, when its expiry date is close or when it must be replaced (without modification of the data of the Subject).

A certificate cannot be re-keyed after its expiration date, and a new issuance of the certificate must be made instead.

For electronic seal, code signing, TSU, CA, and OCSP certificates, no re-key is made, but new issuance of the certificates is made.

3.3.1 IDENTIFICATION AND AUTHENTICATION FOR ROUTINE RE-KEY

The identification and authentication for a re-key request is made through the valid certificate to be re-keyed or based on a pre-existing relationship.

In both cases, the data of the Subject/Signatory in the certificate must not have changed (EXCEPTION: in cases of re-key of a certificate when its expiry date is close and in some cases of certificate replacement, it is allowed to change the email address contained in the certificate) and, in the case of a qualified certificate, the identification of the Subject/Signatory must have been carried out in person less than five years ago. If this is not met, a new issuance of the certificate must be made instead.

3.3.2 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY AFTER REVOCATION

Once a certificate has been revoked, it cannot be re-keyed, and a new issuance of the certificate must be made instead.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

The identification and authentication for a revocation or suspension request or for a report of events which may indicate the need to revoke certificates is performed, for each of the procedures available for the different types of certificates, in accordance with the provisions of section 4.9.3.

Camerfirma, or any of their RAs, may, on its own initiative, request the revocation or suspension of a certificate

- if it is aware or suspects that the Subject's private key has been compromised,
- or if it is aware or suspects of any other event that would make taking such action advisable.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

Camerfirma uses its platforms for lifecycle management for end entity certificates under these CPS and CPs.

This platforms allow performing the actions related to application, application processing, issuance, acceptance, re-key, revocation and suspension of end entity certificates.

The services of this platforms are available 24 hours a day, 7 days a week.

In the event of a system failure, or any other circumstance out of Camerfirma's control, Camerfirma shall apply best endeavours to ensure that these services are not unavailable for longer than 24 hours.

4.1 CERTIFICATE APPLICATION

4.1.1 WHO CAN SUBMIT A CERTIFICATE APPLICATION

A certificate application can be submitted by the Applicant, with the participation, if applicable, of the Person Responsible, and/or the Subject, and/or the Subscriber or the Entity.

4.1.2 ENROLLMENT PROCESS AND RESPONSIBILITIES

4.1.2.1 WEB FORMS

Certificate requests are submitted via the application forms on the Camerfirma website or by sending the Applicant or the Person Responsible a link to a specific form.

Camerfirma 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 Subject has created the keys on an external device not managed by Camerfirma.

After confirmation of the application data, the Person Responsible, and the Subject if they are different, receive an email sent to the account associated with the certificate application containing a link to confirm the application and accept the Terms and Conditions.

Once the application is confirmed, the Applicant 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 TSU certificates must be made formally through the application for a sales quotation and, in the case of TSU certificates, be subsequently incorporated into the application forms.

There are special procedures where the registry operator delivers the conditions of use to the Applicant or the Person Responsible on paper or by email.

4.1.2.2 BATCHES

The platforms also allow batch request circuits. In this case, the Subscriber or the Entity sends the RA a file with a structure designed by Camerfirma containing the Subjects' details. The RA uploads these requests in the management application.

4.1.2.3 APPLICATIONS FOR EXTERNAL TSU AND SUBORDINATE CA CERTIFICATES

Applications for issuing external TSU or Subordinate CA certificates 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 generation event meets the requirements of the corresponding TSU CP in this document, or the requirements of Subordinate CA under the corresponding issuer CA in this CPS.

When the customer generates the cryptographic keys in an HSM device using its resources, Camerfirma collects the necessary evidence, for which it requests a signed report of key generation event, in accordance with the requirements set out in ETSI EN 319 421 (TSU certificates) or ETSI EN 319 411-1 (Subordinate CA certificates), indicating at least the following:

- The procedure followed to generate the keys.
- The people involved.
- The environment in which it was created.
- The HSM device used (make and model).
- Where applicable, HSM configuration to be operated in accordance with FIPS 140-2 level 3 or FIPS 140-3 level 3 or CC EAL 4 or higher.
- Security policy employed: size of keys, key generation parameters, exportable/not exportable and any other relevant information.
- The generated PKCS #10 request, or its hash.
- Any incidents and solutions.

This information is included by the issuer CA 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 and revocation services. Calls to these WS are signed with a certificate recognized by the platform.

Before beginning the issuance using this system, there must be a favorable Camerfirma technical report, a contract where the RA 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 this CPS and the applicable CPs in this document 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 CERTIFICATE APPLICATION PROCESSING

4.2.1 PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS

End entity certificates:

- Once a certificate has been requested, the RA operator, using access to the certificate management platforms, shall verify that the information provided is consistent.
- The RA operator securely accesses the platforms after passing a training and evaluation process.
- Multi-factor authentication is required prior to accessing the certificate management platforms.

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 through platforms are validated once the Applicant's identity and 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.

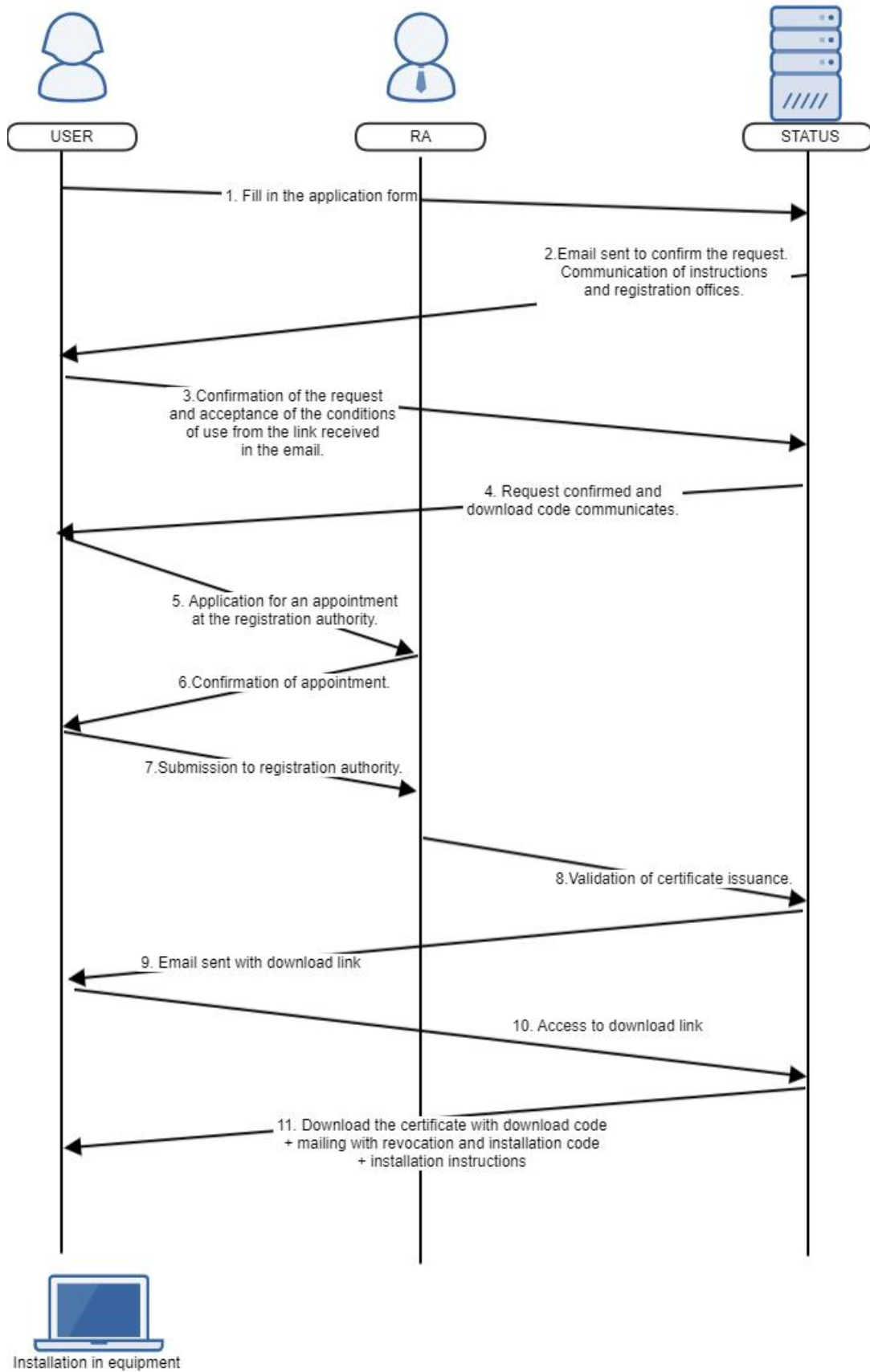
There are no stipulated deadlines for resolving a Subordinate CA certificate or cross-certification application.

4.3 CERTIFICATE ISSUANCE

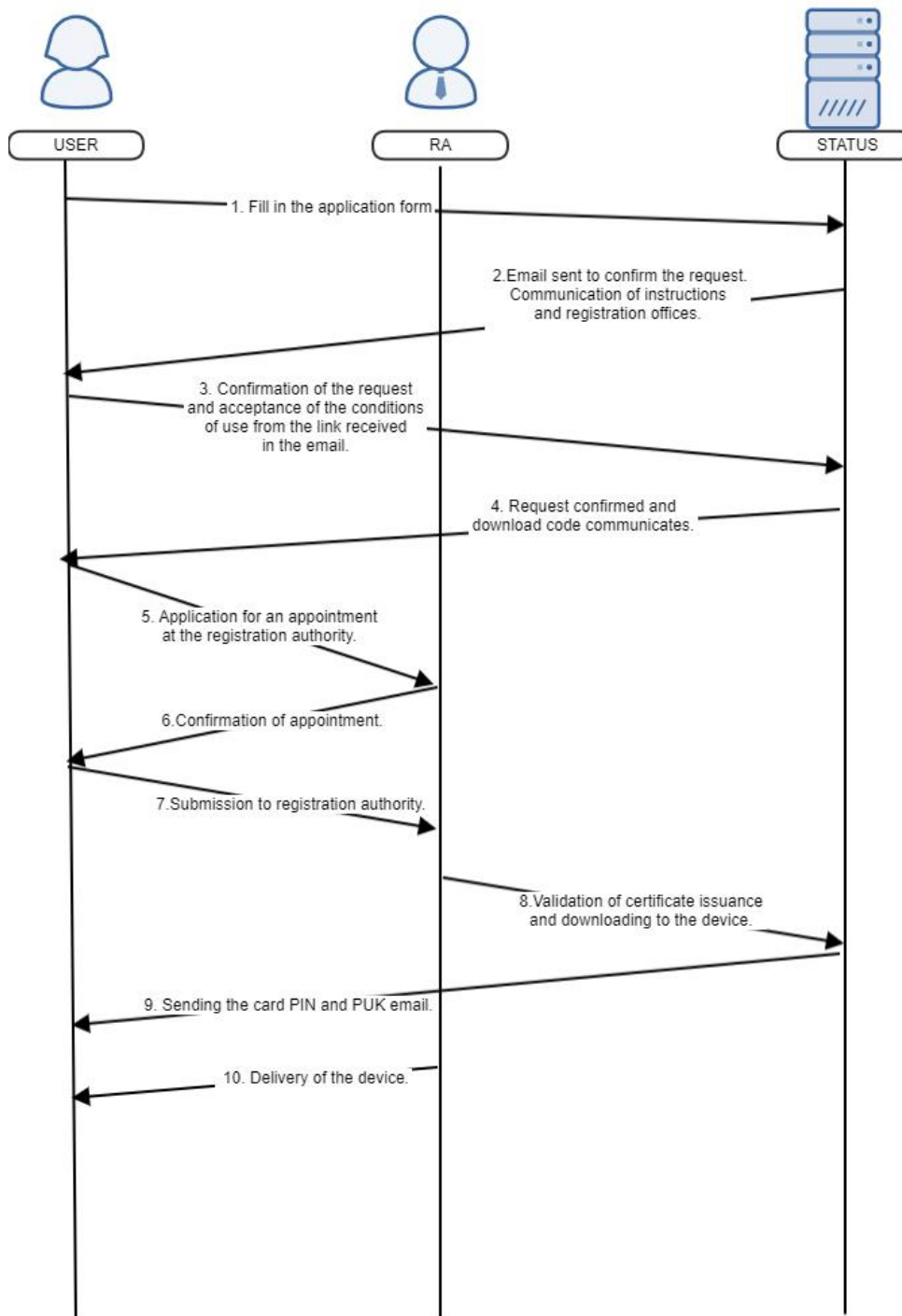
4.3.1 CA ACTIONS DURING CERTIFICATE ISSUANCE

4.3.1.1 CERTIFICATES ON SOFTWARE

Once the application is approved, the Person Responsible 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.



4.3.1.2 CERTIFICATES ON QSCD SMARTCARD/TOKEN OR ON SMARTCARD/TOKEN



The Person Responsible receives the device with the keys and the certificate securely from the RA.

The RA operator chooses which cryptographic smartcard or token type to use to create the keys. For this purpose, the RA operator's workstation is configured with the CSP (Cryptographic Service Provider). Camerfirma currently allows several types of USB cards and tokens, QSCD and Non-QSCD.

For cards, by default the Person Responsible receives the cryptographic device access code and unlocking code, as well as a revocation code, 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 platforms according to section 4.1.2.4.

4.3.1.4 CERTIFICATES ON QSCD CLOUD OR ON CLOUD

Once the application is approved, the Person Responsible receives an email with the notification of this fact and how to proceed to the generation and download of the certificate in the QSCD Cloud or Cloud device (HSM).

If the device is certified as a qualified signature creation or seal creation device (QSCD), the certificate will be issued with the corresponding *QCStatement* in the *Qualified Certificate Statements* extension.

If the device is not certified as a QSCD, or if the device is certified as a QSCD and the certificate is not issued with the corresponding *QCStatement* in the *Qualified Certificate Statements* extension and is not a non-qualified high-level public employee certificate, the certificate shall not contain the OID 1.3.6.1.1.4.1.17326.99.18.1.

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 Person Responsible indicating the approval or denial of the request.

Subordinated CA certificates are issued under the execution of a key ceremony and are subsequently delivered to the Person Responsible.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE

Once the certificate has been delivered, notified or downloaded, the Subject 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

Once the end entity certificate has been delivered, notified or downloaded, it will be entered into the internal certificate registry and will not be made public by the CA, except for OCSP certificates and TSU certificates owned by Camerfirma (see section 2.2.3).

4.4.3 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

Certificates of Camerfirma TSUs issuing qualified electronic time stamps certificates are notified to the national Supervisory Body for incorporation into the TSL.

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

Certificates of Camerfirma Subordinate CAs issuing qualified certificates are notified to the national Supervisory Body for incorporation into the TSL.

If applicable, Root CA and Subordinate CA certificates are notified to an information repository managed by Mozilla, which incorporates information on Certification Authorities - CCADB. This database is used by various commercial programs to manage trusted stores.

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: *Key Usage*, *Extended Key Usage* and *Basic Constraints*.

CA/CP	Key Usage	Extended Key	Basic
-------	-----------	--------------	-------

		Usage	Constraints
CHAMBERS OF COMMERCE ROOT - 2016	critical, cRLSign, keyCertSign	-	critical, CA:true
AC CAMERFIRMA FOR NATURAL PERSONS - 2016	critical, cRLSign, keyCertSign	emailProtection clientAuth	critical, CA:true, pathLen:2
Qualified Citizen Certificate - QSCD SmartCard/Token, QSCD Cloud, Non-QSCD	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical, CA:false
Qualified Corporate Certificate / Qualified Certificate for a Self-employed / Qualified Certificate for a Chartered Self-employed - QSCD SmartCard/Token, QSCD Cloud, Non-QSCD	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical, CA:false
Qualified Certificate for a Legal Representative of a Legal/Non-Legal Entity – QSCD SmartCard/Token, QSCD Cloud, Non-QSCD	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical, CA:false
Qualified Certificate for a Voluntary Representative of a Legal/Non-Legal Entity before the Public Administrations - QSCD SmartCard/Token, QSCD Cloud, Non-QSCD	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical, CA:false
Qualified Certificate for a Special Representative of a Legal/Non-Legal Entity - QSCD SmartCard/Token, QSCD Cloud, Non-QSCD	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical, CA:false
Qualified Certificate for Signature for a Public Employee With/Without a Pseudonym - High Level - QSCD SmartCard/Token, QSCD Cloud	critical, contentCommitment	-	critical, CA:false
Non-Qualified Certificate for Authentication for a Public Employee With/Without a Pseudonym - High Level -	critical, digitalSignature	emailProtection clientAuth	critical, CA:false

SmartCard/Token, Cloud			
Non-Qualified Certificate for Encipherment for a Public Employee With/Without a Pseudonym - High Level - SmartCard/Token, Cloud	critical, keyEncipherment, dataEncipherment	emailProtection clientAuth	critical, CA:false
Qualified Certificate for a Public Employee With/Without a Pseudonym - Medium Level - QSCD SmartCard/Token / Non-QSCD, QSCD Cloud	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 Certificate for Electronic Seal - QSCD SmartCard/Token, Non-QSCD	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical, CA:false
Qualified Certificate for Electronic Seal for Public Administrations - High Level - QSCD SmartCard/Token	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical, CA:false
Qualified Certificate for Electronic Seal for Public Administrations - Medium Level - Non-QSCD	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical, CA:false
AC CAMERFIRMA TSA - 2016	critical, cRLSign, keyCertSign	timeStamping	critical, CA:true, pathLen:2
TSU Qualified Certificate - QSCD HSM	critical, contentCommitment	critical, timeStamping	critical, CA:false
Chambers of Commerce Root – 2008 (certificate SHA -1)	critical, cRLSign, keyCertSign	-	critical, CA:true, pathLen:12
Chambers of Commerce Root – 2008 (certificate SHA -256)	critical, cRLSign, keyCertSign	-	critical, CA:true, pathLen:12
Camerfirma TSA II - 2014	critical, cRLSign, keyCertSign	timeStamping	critical, CA:true, pathLen:2
TSU Non-Qualified Certificate - HSM	critical, digitalSignature, contentCommitment	critical, timeStamping	critical, CA:false

Camerfirma Codesign II - 2014	critical, cRLSign, keyCertSign	codeSigning msCodeCom	critical, CA:true, pathLen:2
Code Signing Non-Qualified Certificate	critical, digitalSignature, nonRepudiation	codeSigning msCodeCom	critical, CA:false
Camerfirma Corporate Server II - 2015	critical, cRLSign, keyCertSign	emailProtection clientAuth serverAuth	critical, CA:true, pathLen:2
Non-Qualified Certificate for Electronic Seal - P12, P10	critical, digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement	clientAuth emailProtection	critical, CA:false
Camerfirma AAPP II - 2014	critical, cRLSign, keyCertSign	emailProtection clientAuth serverAuth	critical, CA:true, pathLen:2
Non-Qualified Certificate for Electronic Seal for Public Administrations	critical, digitalSignature, contentCommitment, keyEncipherment, dataEncipherment	clientAuth emailProtection	critical, CA:false
Non-Qualified Certificate for Electronic Seal for Personnel for Public Administrations	critical, digitalSignature, contentCommitment, keyEncipherment, dataEncipherment	clientAuth emailProtection	critical, CA:false
GLOBAL CHAMBERSIGN ROOT - 2016	critical, cRLSign, keyCertSign	-	critical, CA:true
AC CAMERFIRMA COLOMBIA - 2016	critical, cRLSign, keyCertSign	-	critical, CA:true, pathLen:2
AC CAMERFIRMA PERÚ - 2016	critical, cRLSign, keyCertSign	-	critical, CA:true, pathLen:2
CAMERFIRMA ROOT 2021	critical, cRLSign, keyCertSign	-	critical, CA:true
AC CAMERFIRMA QUALIFIED CERTIFICATES – 2021	critical, cRLSign, keyCertSign	emailProtection, clientAuth	critical, CA:true, pathLen:0
Qualified Citizen Certificate - QSCD	critical,	emailProtection,	critical, CA:false

SmartCard/Token, QSCD Cloud	digitalSignature, contentCommitment, keyEncipherment	clientAuth	
Qualified Corporate Certificate - QSCD SmartCard/Token, QSCD Cloud	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection, clientAuth	critical, CA:false
Qualified Certificate for a Legal Representative of a Legal Entity - QSCD SmartCard/Token, QSCD Cloud	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection, clientAuth	critical, CA:false
Qualified Certificate for a Legal Representative of a Non-Legal Entity - QSCD SmartCard/Token, QSCD Cloud	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection, clientAuth	critical, CA:false
Qualified Certificate for a Voluntary Representative of a Legal Entity before the Public Administrations - QSCD SmartCard/Token, QSCD Cloud	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection, clientAuth	critical, CA:false
Qualified Certificate for a Voluntary Representative of a Non- Legal Entity before the Public Administrations - QSCD SmartCard/Token, QSCD Cloud	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection, clientAuth	critical, CA:false
Qualified Certificate for a Special Representative of a Legal Entity - QSCD SmartCard/Token, QSCD Cloud	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection, clientAuth	critical, CA:false
Qualified Certificate for a Special Representative of a Non-Legal Entity - QSCD SmartCard/Token, QSCD Cloud	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection, clientAuth	critical, CA:false
Non-Qualified OCSP Certificate	critical, digitalSignature, nonRepudiation	OCSPSigning	critical, CA:false
INFOCERT-CAMERFIRMA CERTIFICATES 2024	critical, cRLSign, keyCertSign	-	critical, CA:true
INFOCERT-CAMERFIRMA	critical, cRLSign,	Adobe Trust,	critical, CA:true,

QUALIFIED CERTIFICATES - 2024	keyCertSign	clientAuth	pathLen:0
Qualified Citizen Certificate - Non-QSCD	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical, CA:false
INFOCERT-CAMERFIRMA TIMESTAMP 2024	critical, cRLSign, keyCertSign	-	critical, CA:true
INFOCERT-CAMERFIRMA QUALIFIED TSA - 2024	critical, cRLSign, keyCertSign	timeStamping	critical, CA:true, pathLen:0
TSU Qualified Certificate - QSCD HSM	critical, contentCommitment	critical, timeStamping	critical, CA:false

Although data encryption with certificates is technically possible, Camerfirma is not responsible for any resulting damages should the Subject 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 the Subject / Creator of a Seal must securely retain the remote signature authentication tools and/or devices. It must also keep the private key activation PIN of the remote signature certificate under its sole control (or under its control, in the case of remote seal certificates) and separately from authentication passwords or authentication devices. Finally, it must ensure that it maintains the privacy and preservation of the certificate revocation PIN. The Subject/Signer and the Subject / Creator of a Seal must 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

Relying Parties must use the public key and the certificate as stipulated in these CPS and CPs and as indicated in the Terms and Conditions.

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

4.6 CERTIFICATE RENEWAL

Certificate renewal (without new keys) is not allowed.

4.6.1 CIRCUMSTANCE FOR CERTIFICATE RENEWAL

No stipulation.

4.6.2 WHO MAY REQUEST RENEWAL

No stipulation.

4.6.3 PROCESSING CERTIFICATE RENEWAL REQUESTS

No stipulation.

4.6.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

No stipulation.

4.6.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RENEWAL CERTIFICATE

No stipulation.

4.6.6 PUBLICATION OF THE RENEWAL CERTIFICATE BY THE CA

No stipulation.

4.6.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

No stipulation.

4.7 CERTIFICATE RE-KEY

The re-key of a certificate is the process that must be carried out to obtain a new key pair and a new certificate before its expiry date, when its expiry date is close or when it must be replaced (without modification of the data of the Subject).

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

4.7.1 CIRCUMSTANCE FOR CERTIFICATE RE-KEY

Where allowed, a certificate can be re-keyed before its expiry date.

The certificate re-key is not allowed for:

- Certificates for electronic seal and code signing. New issuance of certificates must be made.
- TSU certificates. New issuance of certificates must be made, no later than 1 year before their expiry date.
- Root CA and Subordinate CAs certificates. New issuance of certificates must be made in a new procedure, through a ceremony created for this purpose, ensuring that the life of the certificate is always longer than the maximum validity period of certificates issued under its hierarchical branch. See section 5.6.
- OCSP certificates. New issuance of certificates must be made periodically, no later than 1 year before their expiry date.

In the following cases the re-key of a certificate is not allowed, and a new issuance of the certificate must be made instead:

- The certificate has expired.
- The certificate has been revoked.
- The data of the Subject/Signatory in the certificate has changed. EXCEPTION: in cases of re-key of a certificate when its expiry date is close and in some cases of certificate replacement, it is allowed to change the email address contained in the certificate.
- In the case of a qualified certificate, more than 5 years have elapsed since the last identification of the Applicant in person.

4.7.2 WHO MAY REQUEST CERTIFICATION OF A NEW PUBLIC KEY

Certificate re-key can be requested by:

- The Subject/Signatory, when the expiry date of the certificate is close and in some cases of certificate replacement (without modification of the data of the Subject).
- The RA through which the certificate was issued, in some cases of certificate replacement (without modification of the data of the Subject).
- The CA (Camerfirma), in some cases of certificate replacement (without modification of the data of the Subject).

4.7.3 PROCESSING CERTIFICATE RE-KEYING REQUESTS

Before re-keying a certificate, it is checked that the data of the Subject/Signatory in the certificate has not changed. If any of the data of the Subject/Signatory in the certificate has changed, a new issuance process must be performed and, if necessary, the old certificate must be revoked. EXCEPTION: in cases of re-key of a certificate when its expiry date is close, it is allowed to change the email address contained in the certificate.

In the case of re-key of qualified certificates, the issuance of a certificate without face-to-face identification of the Subject/Signatory is allowed for a period of 5 years from the last face-to-face identification. Once 5 years have elapsed, the Subject/Signatory must carry out a new issuance process.

The technical process of issuing the certificate at re-keying is the same as when a new issuance is made.

The re-key process for a certificate when its expiry date is close is initiated from the expiry notice email or directly via the following Camerfirma website:

<https://www.camerfirma.com/ayuda/utilidades/renovacion-de-certificados/>

This process requires the use of the private key associated with the valid certificate to be re-keyed.

- Once identified with the certificate to be re-keyed, the application shows the Subject/Signatory the data contained in the old certificate and requests confirmation of this data. If any of the data contained in the certificate has changed, a new issuance process must be performed and, if necessary, the old certificate must be revoked. EXCEPTION: the application allows the Subject/Signatory to change the email address assigned to the certificate.
- The request is registered in the RA application where the operator, after checking the data, proceeds to request the issuance of the certificate to the CA.

In some cases of certificate replacement, the re-key process is initiated from an email sent to the Subject/Signatory. This process requires the use of the private key associated with the valid certificate to be re-keyed.

- Once identified with the certificate to be re-keyed, the application shows the Subject/Signatory the data contained in the old certificate and requests confirmation of this data. If any of the data contained in the certificate has changed, a new issuance process must be performed and, if necessary, the old certificate must be revoked. EXCEPTION: in some cases of certificate replacement, the application allows the Subject/Signatory to change the email address assigned to the certificate.
- The request is registered in the RA application where the operator, after checking the data, proceeds to request the issuance of the certificate to the CA.
- The CA issues the new certificate, taking the same time of re-keying as the start of validity of the new certificate,
- Subsequently, if necessary, the old certificate is revoked.

In other cases of certificate replacement, the re-key process is performed by an operator of the RA through which the certificate was issued or by an operator of the CA. This process does not require the use of the private key associated with the valid certificate to be re-keyed.

- The request is registered in the RA application where the operator, after checking the data, proceeds to request the issuance of the certificate to the CA. If any of the data contained in the certificate has changed, a new issuance process must be performed and, if necessary, the old certificate must be revoked.

- The CA issues the new certificate, taking the same time of re-keying as the start of validity of the new certificate,
- Subsequently, if necessary, the old certificate is revoked.

4.7.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

As stipulated in section 4.3.2.

4.7.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RE-KEYED CERTIFICATE

As stipulated in section 4.4.1.

4.7.6 PUBLICATION OF THE RE-KEYED CERTIFICATE BY THE CA

As stipulated in section 4.4.2.

4.7.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

As stipulated in section 4.4.3.

4.8 CERTIFICATE MODIFICATION

Any need for modification of data of the Subject in a certificate requires a new certificate application. A new certificate will be issued with new keys and corrected data and, if necessary, the old certificate will be revoked.

EXCEPTION: in very specific cases of CA or TSU certificates (for example, in case of change of the signature hash algorithm of the certificate), the new certificate may be allowed to have the same keys as the old certificate, as long as the end of the validity period of the new certificate is no longer than the end of the validity period of the old certificate.

4.8.1 CIRCUMSTANCE FOR CERTIFICATE MODIFICATION

No stipulation.

4.8.2 WHO MAY REQUEST CERTIFICATE MODIFICATION

No stipulation.

4.8.3 PROCESSING CERTIFICATE MODIFICATION REQUESTS

No stipulation.

4.8.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

No stipulation.

4.8.5 CONDUCT CONSTITUTING ACCEPTANCE OF MODIFIED CERTIFICATE

No stipulation.

4.8.6 PUBLICATION OF THE MODIFIED CERTIFICATE BY THE CA

No stipulation.

4.8.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

No stipulation.

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.

If a certificate is revoked, it is invalidated before its expiration date. Any signatures created with it after its revocation becomes effective is invalidated.

The revocation of a certificate is definitive and therefore irreversible.

Suspension, on the other hand, refers to revocation with reason suspension (i.e. a specific revocation case). In this case, a certificate is revoked as a precautionary measure until it is decided whether it should be revoked definitively or reactivated.

The revocation or suspension of a certificate becomes effective from the moment it is included in certificate status services of the issuer CA (publication of CRL or OCSP service).

Revoked or suspended certificates cannot be used under these CPS and CPs.

4.9.1 CIRCUMSTANCES FOR REVOCATION

A certificate will be revoked due to:

General circumstances affecting the information contained in the certificate:

- Errors or incomplete data detected in the data submitted in the certificate request and contained in the certificate.
- Errors or incomplete data detected in any other data contained in the certificate.
- Changes to the circumstances verified for issuing the certificate and contained in the certificate.
- Modification of any other data contained in the certificate.

Circumstances affecting key or certificate security:

- The private key or infrastructures or systems belonging to the CA that issued the certificate are compromised, whenever this incident affects the reliability of the issued certificates.
- The CA or the RA has breached the requirements in the certificate management procedures established in these CPS and CPs.
- Security of the private key or certificate is compromised or suspected of being compromised, including in the event that it is found that the cryptographic mechanisms used to generate the private key or the certificate do not meet the minimum security standards necessary to guarantee its security.
- There is unauthorized third-party access or use of the private key.
- There is a lack of diligence in keeping the private key secure by the Subject or by the Person Responsible.
- There is a misuse of the certificate by the Subject or by the Person Responsible.

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 of the cryptographic device.
- There is loss of the activation data of the private key in the cryptographic device.
- There is unauthorized third-party access to the activation data of the private key in the cryptographic device.
- There is a lack of diligence in keeping the cryptographic device and/or the activation data of the private key in the cryptographic device secure by the Subject or by the Person Responsible.
- Non-compliance by the Subject or by the Person Responsible of the rules of use of the cryptographic device established in these CPS and CPs or in the Terms and Conditions.

Circumstances affecting the Subscriber, the Subject, the Applicant, the Person Responsible or the Entity:

- The relationship is terminated between the CA and the Subscriber.
- There are changes to or termination of the underlying legal relationship or cause for issuing the certificate to the Subject.

- The Subscriber, the Subject, the Applicant, the Person Responsible or the Entity breach part of the requirements established for requesting the certificate.
- The Subscriber, the Subject, the Applicant, the Person Responsible or the Entity breach part of their obligations, responsibility and guarantees established in these CPS and CPs or in the Terms and Conditions.
- The sudden capacity modified by court order or incapacity, total or partial, or death of the Subject/Signatory.
- The termination of the legal or non-legal Entity.
- The Subscriber indicates that the certificate request was not authorized and that does not grant the authorization retroactively.
- The authorization provided by the Subscriber to the Subject has been cancelled or has expired.
- In the case of certificates issued to legal persons, the authorization provided by the Subscriber to the Person Responsible has been cancelled or the relationship between the Subject and the Person Responsible has finished, where the Person Responsible still has, or is suspected of having, access to the private key.
- The revocation is requested by the Subject, the Subscriber, the Entity, or an authorized third party.
- In case the Applicant, the Subject/Signatory, or the Person Responsible request to modify or delete his/her data from Camerfirma registers.

Circumstances affecting compliance with applicable regulations:

- The certificate was issued in non-compliance with the requirements established in the version of these CPS and CPs and/or the Terms and Conditions in force at the time of issuance of the certificate.
- The certificate was issued with non-compliance with the requirements established in the applicable legal regulations and/or in the version of the applicable ETSI standards (see section 1.1) in force at the time of certificate issuance.
- The certificate no longer complies with the requirements established in the version of these CPS and CPs and/or the Terms and Conditions, and/or in the applicable legal regulations and/or in the version of the applicable ETSI standards in force at the time of certificate issuance, by subsequent changes to the circumstances verified for the issuance of the certificate, for example, because the cryptographic device is no longer certified as a qualified signature creation or seal creation device (QSCD), and the certificate is issued with the corresponding *QCStatement* in the *Qualified Certificate Statements* extension.

Other circumstances:

- Failure to pay for the certificate.
- Firm resolution of the competent administrative or judicial authority.

- Suspension of the certificate for a longer period than established in this CPS (see section 4.9.16).
- Cessation of Camerfirma's activity as a TSP (see section 5.8.1).
- Termination of the CA (see section 5.8.2).
- If applicable, termination of the RA (see section 5.8.3).
- Any other circumstances specified in these CPS and CPs or in the Terms and Conditions.
- Any other circumstances specified in the applicable legal regulations and/or ETSI standards (see section 1.1).

The revocation process does not apply to Root CA certificates.

4.9.2 WHO CAN REQUEST REVOCATION

Certificate revocation can be requested by:

- The Person Responsible.
- The Subject.
- The Subscriber.
- The Entity.
- An authorized third party.
- The RA through which the certificate was issued.
- The CA (Camerfirma).

Any interested person may report the RA or the CA events which may indicate the need to revoke a certificate.

4.9.3 PROCEDURE FOR REVOCATION REQUEST

Certificate revocation can be requested using one of the following procedures:

1) Online revocation service.

This procedure is available for all types of end entity certificates, except TSU and OCSP certificates.

The revocation will be requested via the online revocation service located on the following Camerfirma website, by entering the certificate revocation PIN and the email address to which it was delivered, and selecting the reason for revocation (it can be "unspecified"):

<https://www.camerfirma.com/ayuda/utilidades/revocacion-de-certificados/>

The initial certificate revocation PIN is delivered to the Person Responsible at the email

address declared in the certificate application form, during the certificate issuance process.

If requested by the Subject, a new certificate revocation PIN will be delivered to the Subject at the email address declared in the certificate application form.

The applicant for revocation may be the Person Responsible, the Subject, or any of the others set out in section 4.9.2, if, as agreed between them, the Person Responsible or the Subject informs them of the certificate revocation PIN and the email address to which it has been sent, or if they have access to the email address to which the revocation PIN has been sent.

Camerfirma will store the corresponding online revocation service audit logs, as evidence of the revocation request.

This is the main revocation request procedure for all types of end entity certificates, except for TSU certificates, which guarantees that Camerfirma will register the certificate revocation in its certificate database and publish the revocation status of the certificate (via CRL and OCSP) in a period of much less than 24 hours after the receipt of the request, in accordance with the provisions of the eIDAS Regulation regarding the revocation of qualified certificates.

2) Request sent to a Camerfirma web service.

This procedure will only be available under specific projects.

The request must contain the data identifying the certificate or certificates to be revoked and, optionally, the corresponding reason for revocation.

The request must be digitally signed with an active qualified certificate issued by Camerfirma to the revocation applicant, which may be:

- The Entity (legal person): the certificate used must be a certificate issued by Camerfirma to the Entity, under one of the CPs Qualified Certificate for Electronic Seal or Qualified Certificate for Electronic Seal for Public Administrations in this document.
- A third party (natural person) authorized to request revocation on behalf of the Entity: the certificate used must be a certificate issued by Camerfirma to the Entity's legal representative, under one of the PC Qualified Certificate for a Legal Representative of a Legal/Non-Legal Entity in this document.

Camerfirma will store the digitally signed request received and the corresponding web service audit logs, as evidence of the revocation request.

3) Revocation request document sent to the RA through which the certificate was issued or to the CA (Camerfirma).

This procedure is available for:

- In the case of sending the request document to the RA, all types of end entity certificates, except TSU and OCSP certificates.
- In the case of sending the request document to the CA, all types of end entity certificates, except Camerfirma OCSP certificates, and certificates of external Subordinate CAs.

The request document must contain the data identifying the certificate or certificates to be revoked and, optionally, the corresponding reason for revocation.

The request document must specify that revocation is requested during public opening hours.

The application document must be digitally signed with a valid certificate issued by the same CA (the same certificate to be revoked or another certificate) or by another Camerfirma CA, with a valid qualified certificate issued by another QTSP, or with a valid certificate issued by another CA trusted by the RA or the CA, or with an original handwritten signature (not scanned), by the revocation applicant, which may be:

- For revocation requests for end entity certificates issued to natural persons without attributes of association with an Entity: the Person Responsible and Subject, the Subscriber, or an authorized third party.
- For revocation requests for end entity certificates issued to natural persons with attributes of association with an Entity: the Person Responsible and Subject, the Subscriber, the Entity, or an authorized third party.
- For revocation requests for end entity certificates issued to legal persons, except TSU certificates: the Person Responsible, the Subscriber and Entity, or an authorized third party.
- For revocation requests for TSU and external Subordinate CA certificates: the Subscriber and Entity, or an authorized third party.

In the case that the signature on the request document is handwritten, the RA or CA operator who processes the request will verify its authenticity by checking it against another handwritten signature and/or confirmation from the revocation applicant.

The RA or the CA will store the request document received and record the date and time of its receipt during public opening hours, as evidence of the revocation request.

- 4) Physical presence of the applicant at an office of the RA through which the certificate was issued or the CA (Camerfirma) during public opening hours.

This procedure is available, in cases of physical presence of the applicant at an office of the RA appearance at a RA or CA office, for all types of end entity certificates, except TSU and OCSP certificates.

The applicant for revocation must identify himself/herself to an RA or CA operator with a valid identity document (National Identity Card, passport or other legally accepted means).

The request document must indicate the data identifying the certificate or certificates to be revoked and, optionally, the corresponding reason for revocation.

The applicant for revocation who is in person may be:

- For revocation requests for end entity certificates issued to natural persons without attributes of association with an Entity: the Person Responsible and Subject, or a third party (natural person) authorized to request the revocation on behalf of the Person Responsible and Subject, or the Subscriber.

- For revocation requests for end entity certificates issued to natural persons with attributes of association with an Entity: the Person Responsible and Subject, or a third party (natural person) authorized to request the revocation on behalf of the Person Responsible and Subject, the Subscriber, or the Entity.
- For revocation requests for end entity certificates issued to legal persons: a third party (natural person) authorized to request the revocation on behalf of the Subject, or the Subscriber and Entity.

The RA or the CA will store the photocopied or scanned identity document of the applicant and will register the date and time of the physical presence of the applicant, as evidence of the revocation request.

- 5) Revocation request made by the RA through which the certificate was issued or the CA (Camerfirma).

This procedure is the only procedure for revocation request that is also available to request the suspension of a certificate and, if applicable, to request its subsequent reactivation.

This procedure is available for:

- In the case of a request for revocation, suspension or reactivation made by the RA, all types of end entity certificates, except TSU and OCSP certificates.
- In the case of a request for revocation made by the CA, all types of end entity certificates, including TSU and OCSP certificates, certificates of Subordinate CAs under this CPS and external Subordinate CAs.
- In the case of a request for suspension or reactivation made by the CA, all types of end entity certificates, except TSU and OCSP certificates.

For revocation, suspension or reactivation requests for end entity certificates, except for Camerfirma OCSP certificates issued by Root CAs and offline Subordinate CAs under this CPS:

- An authorized operator (trusted role *Revocation Officers*) of the RA or the CA will request the revocation, suspension or reactivation of the certificate on the certificate management platforms. The certificate may be revoked, suspended or reactivated:
 - Individually, by selecting on the platforms the certificate to be revoked, suspended or reactivated and, where applicable, the reason for revocation (it can be "unspecified"). The certificate revocation, suspension or reactivation is performed immediately.
 - Together with other certificates (only available for revocation requests), by uploading to the platforms a batch with the identifiers of the certificates to be revoked and selecting the revocation reason (it can be "unspecified") for all of them. The revocation of all the certificates identified in the batch is performed later at a scheduled time.

Camerfirma will store the corresponding audit logs of the certificate management platforms, as evidence of the revocation, suspension or reactivation request.

- Alternatively, where applicable, an authorized operator (trusted role *Revocation Officers*) of a Remote RA (see section 1.3.2) can request the certificate revocation on a third party application that communicates, via integration with a web services layer, with the certificate management platforms (see section 4.1.2.4).
 - The certificate will be revoked individually, by selecting on the third party application the certificate to be revoked and, if applicable, the reason for revocation (it can be "unspecified"). The certificate revocation will be performed immediately.

The Remote RA will store the corresponding audit logs of the third party application platform, as evidence of the revocation request.

Camerfirma will store the corresponding audit logs of the certificate management platforms, as evidence of the revocation request.

For revocation requests for Subordinate CA certificates and Camerfirma OCSP certificates issued by Root CAs and offline Subordinate CAs under this CPS:

- The participation of two authorized operators (trusted role *Revocation Officers*) of the CA will be required to execute a specific process on the platform of the CA that issued the certificate. The certificate revocation will be performed immediately by issuing a CRL by the CA, containing the certificate serial number, the revocation date and time and the reason for revocation specified by the operators.

Camerfirma will register the issuance of the CRL in a report, as evidence of the revocation request.

In the case of revocation of TSU, OCSP and external Subordinate CA certificates, requested using procedures 3) and 5), given the high impact of certificate revocation, Camerfirma will always confirm the revocation request with the certificate Subscriber.

Once the revocation request has been made, and the revocation applicant has been correctly identified and authenticated as indicated in each procedure and, in the case of revocation of TSU and external Subordinate CA certificates, once the request has been confirmed with the certificate Subscriber, the certificate will be revoked as follows:

- Procedures 1), 2) and 5): automatically, with no subsequent participation of an operator.
- Procedures 3) and 4): with subsequent participation of an operator, by means of a request made by the RA or CA, in accordance with procedure 5).

The RA or the CA may request the immediate suspension or revocation of a certificate using procedure 5) unilaterally, for security or non-payment reasons, without the Subscriber or the Subject being entitled to claim any compensation for this fact.

The RA or the CA may, in other cases, agree with the Subject and/or the Subscriber on a future revocation date (see section 4.9.4).

The services of procedures 1), 2) and 5) are available 24 hours a day, 7 days a week.

In the event of a system failure, or any other circumstance out of Camerfirma's control,

Camerfirma shall apply best endeavours to ensure that these services are not unavailable for longer than 24 hours.

Reports of events which may indicate the need to revoke certificates issued under these CPS and CPs can be made by any interested party via oral or written communication with the RA through which the certificate was issued or with the CA (Camerfirma).

The RA or CA operator must check that the report is from an authorized source, that the facts reported are true and that they correspond to one any of the circumstances for revocation set out in section 4.9.1.

The operator may, if necessary, request additional documentation from the person submitting the report that helps to check that the facts reported are true (for example, a death certificate of the Subject/Signatory of a certificate) and/or confirm the facts reported with the Subjects, Subscribers, Entities or authorized third parties of the affected certificates.

Once the operator has carried out all the aforementioned checks, the RA or CA may request the suspension or revocation of the affected certificates using the aforementioned procedure 5), after having informed their respective Subscribers and Subjects.

4.9.4 REVOCATION REQUEST GRACE PERIOD

The CA, or any of their RAs, may grant a revocation request grace period in specific cases that require a future revocation date, for example:

- Revocation request made using the procedure of revocation request document sent to the RA through which the certificate was issued or to the CA (Camerfirma), as specified in procedure 3) in section 4.9.3.
- Revocation of a TSU or Subordinate CA or OCSP certificate scheduled for a specific date agreed with the Subscriber.
- Modification or termination of the underlying legal relationship or cause for issuing the certificate to the Subject scheduled for a specific date.
- Period for replacement of the certificate prior to its revocation agreed with the Subject and/or the Subscriber.
- The cryptographic device where the certificate keys have been generated will be no longer certified on a certain date as a qualified electronic signature or seal creation device (QSCD) and the certificate contains the corresponding QCStatement in the Qualified Certificate Statements extension.
- Revocation of all active certificates issued by a CA under this CPS, in case of termination of the CA (see section 5.8.2).

In these cases, the scheduled revocation date shall be considered and the UTC time 08:00 as the time at which receipt of the request has occurred and, if applicable, the revocation request may be cancelled or its revocation date postponed before this date and time, by decision of the Subject and/or the Subscriber, or by Camerfirma's decision accepted by the Subject and/or the Subscriber.

4.9.5 TIME WITHIN WHICH CA MUST PROCESS THE REVOCATION REQUEST

Requests for revocation or suspension and reports of events relating to revocation shall be processed on receipt.

In the case of procedures for revocation or suspension request with no subsequent participation of an operator (procedures 1), 2) and 5) specified in section 4.9.3), the decision to change the certificate status information is immediate after the receipt of the request.

In the case of procedures for revocation request with subsequent participation of an operator (procedures 3) and 4) specified in section 4.9.3), the maximum delay between the receipt of the request and the decision to change the certificate status information shall be 23 hours for end entity certificates, except for Camerfirma OCSP certificates issued by Root CAs and offline Subordinate CAs under this CPS, and 12 hours for Subordinate CA certificates and Camerfirma OCSP certificates issued by Root CAs and offline Subordinate CAs under this CPS. If the revocation request cannot be confirmed within this time, then the certificate status need not be changed.

The CA shall immediately process revocation or suspension requests after their confirmation and shall register such revocations or suspensions in its certificate database.

The maximum delay between the processing of a revocation or suspension request by the CA and the actual change of the certificate status information being made available to Relying Parties (through CRL and OCSP) shall be 1 hour for end entity certificates, except for Camerfirma OCSP certificates issued by Root CAs and offline Subordinate CAs under this CPS, and 12 hours for Subordinate CA certificates and Camerfirma OCSP certificates issued by Root CAs and offline Subordinate CAs under this CPS.

Therefore, if an RA or the CA decides to revoke or suspend a certificate, the CA shall register such revocation or suspension in its certificate database and publish the revocation status of the certificate in a timely manner, and in any event within 24 hours after the receipt of the request, in accordance with the provisions of eIDAS Regulation regarding the revocation of qualified certificates.

In the case of reports of events relating to revocation, there is no maximum delay between the receipt of the report and the decision to change the certificate status information, as this time period depends on the indeterminate time required for the operator to check that the report is from an authorized source, that the facts reported are true and that they correspond to one any of the circumstances for revocation set out in section 4.9.1, in accordance with section 4.9.3, but the operator shall apply best endeavours to keep the time as short as possible.

4.9.6 REVOCATION CHECKING REQUIREMENT FOR RELYING PARTIES

Relying Parties must check the status of the certificates issued by CAs under this CPS by consulting either the corresponding CRL or the corresponding OCSP service.

4.9.7 CRL ISSUANCE FREQUENCY

CA	Issuance frequency	Validity
CHAMBERS OF COMMERCE ROOT - 2016 Chambers of Commerce Root - 2008	Maximum 1 hour after revocation / Maximum 365 days	365 days
AC CAMERFIRMA FOR NATURAL PERSONS - 2016 AC CAMERFIRMA FOR LEGAL PERSONS – 2016 AC CAMERFIRMA TSA - 2016 Camerfirma TSA II - 2014 Camerfirma Codesign II - 2014 Camerfirma Corporate Server II - 2015 Camerfirma AAPP II – 2014	Immediate after revocation / 24 hours	2 days
GLOBAL CHAMBERSIGN ROOT - 2016 AC CAMERFIRMA COLOMBIA - 2016 AC CAMERFIRMA PERÚ - 2016	Maximum 1 hour after revocation / Maximum 365 days	365 days
CAMERFIRMA ROOT 2021	Maximum 1 hour after revocation / Maximum 365 days	365 days
AC CAMERFIRMA QUALIFIED CERTIFICATES – 2021	1 hour	24 hours
INFOCERT-CAMERFIRMA CERTIFICATES 2024	Maximum 1 hour after revocation / Maximum 365 days	365 days
INFOCERT-CAMERFIRMA QUALIFIED CERTIFICATES -2024	1 hour	24 hours
INFOCERT-CAMERFIRMA TIMESTAMP 2024	Maximum 1 hour after revocation / Maximum 365 days	365 days
INFOCERT-CAMERFIRMA QUALIFIED TSA - 2024	1 hour	24 hours

Under special circumstances, the CA may force the issuance of an unplanned CRL.

4.9.8 MAXIMUM LATENCY FOR CRLS

The maximum time between the issuance and the publication of the CRLs (maximum latency) is:

CA	Maximum latency
CHAMBERS OF COMMERCE ROOT – 2016	12 hours
Chambers of Commerce Root – 2008	
AC CAMERFIRMA FOR NATURAL PERSONS – 2016	3 minutes
AC CAMERFIRMA FOR LEGAL PERSONS – 2016	
AC CAMERFIRMA TSA – 2016	
Camerfirma TSA II – 2014	
Camerfirma Codesign II – 2014	
Camerfirma Corporate Server II – 2015	
Camerfirma AAPP II – 2014	
GLOBAL CHAMBERSIGN ROOT – 2016	12 hours
AC CAMERFIRMA COLOMBIA – 2016	
AC CAMERFIRMA PERÚ – 2016	
CAMERFIRMA ROOT 2021	12 hours
AC CAMERFIRMA QUALIFIED CERTIFICATES – 2021	Immediate
INFOCERT-CAMERFIRMA CERTIFICATES 2024	12 hours
INFOCERT-CAMERFIRMA QUALIFIED CERTIFICATES - 2024	Inmediate
INFOCERT-CAMERFIRMA TIMESTAMP 2024	12 hours
INFOCERT-CAMERFIRMA QUALIFIED TSA - 2024	Inmediate

4.9.9 ON-LINE REVOCATION/STATUS CHECKING AVAILABILITY

All CAs under this CPS provide an OCSP service for online revocation checking for issued certificates, until the termination of the CA for a reason other than the compromise of its private key (see section 5.8.2) or until the cessation of Camerfirma's activity as a TSP (see section 5.8.1).

4.9.10 ON-LINE REVOCATION CHECKING REQUIREMENTS

For online revocation checking for a certificate issued by a CA under this CPS with the OCSP service of the CA:

- Camerfirma shall make the OCSP service available to the Relying Parties with the possibility of using GET and POST methods.
- The OCSP service responses shall be signed with the corresponding OCSP certificate issued by the CA or, in the event of termination of the CA (see section 5.8.2), with a *default* OCSP certificate (see section 1.3.1.3).
- In the event of termination of the CA for a reason other than the compromise of its private key (see section 5.8.2), the OCSP service responses for certificates issued by the CA shall contain the status *unknown*.
- Camerfirma shall update the information provided via the OCSP service within the maximum time indicated in the following table after a certificate issued by the Root CA is revoked (maximum latency).
- The OCSP service responses shall have the validity indicated in the following table.

CA	Maximum latency	Validity
CHAMBERS OF COMMERCE ROOT - 2016	12 hours	1 hour
Chambers of Commerce Root - 2008		
AC CAMERFIRMA FOR NATURAL PERSONS - 2016	10 minutes	1 hour
AC CAMERFIRMA FOR LEGAL PERSONS - 2016		
AC CAMERFIRMA TSA - 2016		
Camerfirma TSA II - 2014		
Camerfirma Codesign II - 2014		
Camerfirma Corporate Server II - 2015		
Camerfirma AAPP II - 2014		
GLOBAL CHAMBERSIGN ROOT - 2016	12 hours	1 hour
AC CAMERFIRMA COLOMBIA - 2016		
AC CAMERFIRMA PERÚ - 2016		
CAMERFIRMA ROOT 2021	12 hours	1 hour
AC CAMERFIRMA QUALIFIED CERTIFICATES – 2021	Immediate	1 hour
INFOCERT-CAMERFIRMA CERTIFICATES 2024	12 hours	1 hour
INFOCERT-CAMERFIRMA QUALIFIED CERTIFICATES - 2024	Immediate	1 hour
INFOCERT-CAMERFIRMA TIMESTAMP 2024	12 hours	1 hour

INFOCERT-CAMERFIRMA QUALIFIED TSA - 2024

Immediate

1 hour

4.9.11 OTHER FORMS OF REVOCATION ADVERTISEMENTS AVAILABLE

When an end entity certificate is revoked, an email notification is sent to the Subject specifying the date and time of revocation and the reason for the revocation.

When an end entity certificate is suspended, an email notification is sent to the Subject specifying the date and time of suspension.

If the suspension does not result in a definitive revocation and the end entity certificate is reactivated, when his happens, an email notification is sent to the Subject specifying the date and time of reactivation.

The date of revocation of a TSU certificate shall be agreed in advance with the Subscriber (see section 4.9.4).

4.9.12 SPECIAL REQUIREMENTS REGARDING PRIVATE KEY COMPROMISE

Any party that detects the compromise of private keys associated with active certificates issued under this CPS, or suspects such compromise, may notify Camerfirma by sending an email to the address incidentes@camerfirma.com with the subject "Key compromise notification", identifying the certificates associated with the compromised private keys.

In the case of compromise of private keys associated with Root or Subordinate CA certificates, Camerfirma shall proceed as established in section 5.7.3.

4.9.13 CIRCUMSTANCES FOR SUSPENSION

As a general rule, a certificate may be suspended due to not fully verified suspicion of one of the circumstances for revocation (see section 4.9.1).

The suspension process does not apply to:

- TSU certificates
- Root CA and Subordinate CA certificates.
- OCSP certificates.
- End entity certificates issued by Subordinate CAs under this CPS within the CAMERFIRMA ROOT 2021 hierarchy (see section 1.3.1.3) and INFOCERT-CAMERFIRMA ROOT 2024 (see section 1.3.1.4)

4.9.14 WHO CAN REQUEST SUSPENSION

Certificate suspension can be requested by:

- The RA.
- The CA (Camerfirma).

4.9.15 PROCEDURE FOR SUSPENSION REQUEST

The request for suspension and, if applicable, the later request for reactivation can only be made using the procedure for revocation request 5) specified in section 4.9.3.

4.9.16 LIMITS ON SUSPENSION PERIOD

The maximum period of suspension of a certificate is 7 calendar days.

Camerfirma supervises, via alert system of certificate management platform, that the suspension period established by these CPS and CPs is not exceeded.

If the maximum suspension period is reached without reactivation or definitive revocation of the certificate, the system will automatically revoke the certificate definitively with the reason "unspecified".

4.10 CERTIFICATE STATUS SERVICES

4.10.1 OPERATIONAL CHARACTERISTICS

Certificate status information is available through CRLs and OCSP services.

The primary certificate status service of CAs under this CPS is the one provided by the OCSP service of each CA.

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

Each Root CA under this CPS, and each Subordinate CA under this CPS within the CHAMBERS OF COMMERCE ROOT hierarchies (see section 1.3.1.1) and the GLOBAL CHAMBERSIGN ROOT hierarchies (see section 1.3.1.2) issues a single CRL. These CRLs maintain the revoked certificates until they have expired. When this occurs, they are removed from the CRL. A certificate will only be removed from a CRL 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.

The remaining Subordinate CAs under this CPS issue one CRL for every 50,000 issued certificates. These CRLs include revoked certificates that have expired, with no time limit after their expiry.

The OCSP services of all CAs under this CPS provide information on the status of certificates that have expired, with no time limit after their expiry.

4.10.2 SERVICE AVAILABILITY

Certificate status services are available 24 hours a day, 7 days a week.

Certificates may contain more than one access address to CRLs to ensure their availability.

In the event of a system failure, or any other circumstance out of Camerfirma's control, Camerfirma shall apply best endeavours to ensure that these services are not unavailable for longer than 24 hours.

In the event of termination of a CA under this CPS (see section 5.8.2):

- The last CRL/s issued by the CA in accordance with section 5.8.2 will be available at the same access addresses, for at least 15 years after the expiry of all the certificates issued by the CA or until the cessation of Camerfirma's activity as a TSP (see section 5.8.1), and, in addition, in the case of Camerfirma CAs, they will be available with their hashes SHA-1 and SHA-256 for the same period of time on the website:

<https://www.camerfirma.com/autoridades-de-certificacion/>

- In case of compromise of the CA's private key (see section 5.7.3), the OCSP service will continue to provide information on the status of certificates issued by the CA, with responses signed with a *default* OCSP certificate (see section 1.3.1.5) until the cessation of Camerfirma's activity as a TSP.
- If there is no compromise of the CA's private key, the OCSP service will no longer provide information on the status of certificates issued by the CA (the service's responses will contain the status *unknown* and will be signed with a *default* OCSP certificate; see section 1.3.1.5).

In the event of cessation of Camerfirma's activity as a TSP, the provision of revocation status information on the certificates issued by Camerfirma's CAs shall be guaranteed by Camerfirma or by a reliable party to whom it transfers this obligation, through the CAs' last CRLs, for at least 15 years after the expiry of all certificates issued by the CAs.

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 and the Subject 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 issued on QSCD SmartCard/Token or on SmartCard/Token, it is the Subject who keeps the private key in the cryptographic smartcard or token delivered by the RA or the CA.

For certificates issued on software, Camerfirma stores the Subject 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 on QSCD Cloud, Camerfirma stores the generated keys for the user in an HSM QSCD, providing the corresponding mechanisms to guarantee the sole control of the private key by the Subject/Signatory, or the control of the private key by the Subject / Creator of a Seal.

For certificates issued on QSCD Cloud, Camerfirma stores the generated keys for the user in an HSM FIPS-140-2 level 3 or CC EAL 4 or higher, providing the corresponding mechanisms to guarantee the sole control of the private key by the Subject/Signatory, or the control of the private key by the Subject / Creator of a Seal.

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.

4.12.2 SESSION KEY ENCAPSULATION AND RECOVERY POLICY AND PRACTICES

No stipulation.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

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

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

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

- 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.

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.

For OCSP 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 and in Ireland Europe Region.

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

5.1.2 PHYSICAL ACCESS

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 authorized 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 authorized 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.

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 authorized people are required to access, store or withdraw devices.

5.2 PROCEDURAL CONTROLS

5.2.1 TRUSTED ROLES

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

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

- Duties associated with the role.
- Access level.
- Monitoring operation.
- Training and awareness.
- Required skills.

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

- *Security Officers*: Overall responsibility for administering the implementation of the security practices.
- *System Administrators*: Authorized to install, configure and maintain the TSP's trustworthy systems for service management. This includes recovery of the system.
- *System Operators*: Responsible for operating the TSP's trustworthy systems on a day-to-day basis (excluding operations for which the trusted roles *Registration Officers* and *Revocation Officers* are responsible). Authorized to perform a system backup.
- *System Auditors*: Authorized to view archives and audit logs of the TSP's trustworthy systems.
- *Registration Officers*: Responsible for verifying information that is necessary for certificate issuance and approval of certification requests.
- *Revocation Officers*: Responsible for operating certificate status changes.

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 Subordinate CA key storage device.

5.2.3 IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE

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

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

5.2.4 ROLES REQUIRING SEPARATION OF DUTIES

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

5.3 PERSONNEL CONTROLS

5.3.1 QUALIFICATIONS, EXPERIENCE, AND CLEARANCE REQUIREMENTS

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.

5.3.2 BACKGROUND CHECK PROCEDURES

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

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

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

5.3.3 TRAINING REQUIREMENTS

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

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.

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.

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.

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 Subject/Signatory for individual certificates or a future key

Subject / Creator of a Seal 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 (in the case of certificate life-cycle events, from the expiry of the certificate).

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 authorized persons.

Devices are always handled by authorized 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.

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 authorized 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 (logs), including CAs, OCSP services, TSUs and QSCD and Non-QSCD centralized platforms, incorporating the signature events performed.
- Any data related to certificates, including contracts with Subscribers, Subjects and the RA, and the data relating to their identification.
- Requests to issue and revoke certificates.
- Type and number of document submitted in the certificate application.
- Identity of the RA that accepts the certificate application.
- Issued certificates.
- Issued CRLs.
- CPS and CPs.

Camerfirma is responsible for correctly filing all this material.

5.5.2 RETENTION PERIOD FOR ARCHIVE

Certificates, contracts with Subscribers, acceptance of the Terms and Conditions, and any information relating to the identification and authentication of the Subject and the Applicant and, where applicable, to the Person Responsible identity must be kept for at least 15 years after the expiration date of any certificate issued based on that information.

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 PROTECTION OF ARCHIVE

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

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 authorized personnel

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.

5.5.6 ARCHIVE COLLECTION SYSTEM (INTERNAL OR EXTERNAL)

No stipulation.

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.

5.6 KEY CHANGEOVER

The change of keys of an end-entity certificate and of an OCSP certificate is performed through the process of a new issuance or, if applicable, through the process of a certificate re-key (see corresponding sections in these CPS and CPs).

The keys of Root CAs and Subordinate CAs shall be changed before the CA certificate expires or, otherwise, the CA shall be terminated (see section 5.8.2).

The keys of Root CAs and SubCAs shall also be changed when there is a change in cryptographic technology (algorithms, key size, etc.) which requires it, or to comply with the requirements of applicable standards and legislation.

To change the keys of a CA, a new certificate of a new CA shall be generated, with a new associated private key and a CN in the *Subject* field different from that of the certificate of the CA to be replaced.

Once the keys of a CA have been changed, the private key of the old CA will only be used to sign CRLs as long as there are active certificates issued by said CA, i.e., signed with the private key of the old CA.

New certificates of Camerfirma Subordinate CAs issuing qualified certificates are notified to the national Supervisory Body for incorporation into the TSL.

If applicable, Root CA and Subordinate CA new certificates are notified 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.

New certificates of Root CAs and Subordinate CAs under this CPS shall be included in the next versions of these CPS and CPs. The corresponding change shall be indicated in the document history of the version in which the new CA certificates are incorporated.

Once the keys of a CA have been changed, the old CA shall be terminated before its certificate expires (see section 5.8.2).

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 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 certificates will be issued.

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

If any equipment is damaged or stops working, but the private keys are not destroyed, normal activity must be restored as quickly as possible, prioritizing the ability to generate certificate status information according to Camerfirma's disaster recovery plan.

5.7.3 ENTITY PRIVATE KEY COMPROMISE PROCEDURES

A CA, Root or Subordinate 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 CA's private key and to all system development and maintenance activities that may have an impact on it.

Although it is a rare event, Camerfirma have set up a detailed procedure to be followed within the ISO 27001 certified ISMS.

Once the compromise of the private key of a CA under this CPS has been ascertained, Camerfirma

shall promptly proceed to:

- If the CA is a Subordinate CA, revoke its certificate/s associated with the compromised private key.
- Inform the national Supervisory Body within the next 24 hours.
- Inform affected RAs, affected customers (Subscribers and Subjects of active end entity certificates issued by the CA, and/or Entities owning external Subordinate CAs with active certificates issued by the CA), Relying Parties and other affected entities with which it has agreements or other types of relationships, through direct communication where possible, and through communication on the Camerfirma website.
- Indicate in the above information:
 - If known, date and time when the compromise of the CA's private key occurred or is suspected to have occurred.
 - That certificates and revocation status information signed with the CA's compromised private key may no longer be valid.
 - Actions taken and/or planned to invalidate the CA's compromised private key (revocation of its associated certificate/s) and to reliably provide revocation status information for certificates issued by the CA.
- Terminate the CA

Once the CA has been terminated in accordance with the provisions of section 5.8.2, Camerfirma shall continue to reliably provide information on the revocation status of certificates issued by the CA, through the last CRL/s and the OCSP service at the same access addresses, without using the compromised private key or an OCSP certificate signed with the compromised private key, as follows:

- The last CRL/s shall be signed with a new private key associated with a new CA certificate with the same *subject* field.

In case of compromise of the private key of a Subordinate CA, the new CA certificate shall be issued by the same issuing CA or by another Camerfirma CA under the same hierarchy.

In case of compromise of a Root CA's private key, the new CA certificate shall be issued by another Camerfirma CA under another Camerfirma hierarchy.

- The OCSP service shall continue to provide information on the status of certificates issued by the CA, but the service's responses will be signed with a *default* OCSP certificate issued by another CA (see section 1.3.1.5).

Camerfirma may replace the CA with the compromised key with a new CA or another existing CA, and offer new certificates issued by this CA to the affected customers.

5.7.4 BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER

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

5.8 CA OR RA TERMINATION

5.8.1 CESSATION OF ACTIVITY

Before Camerfirma ceases its activity as a TSP issuing qualified certificates:

- 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 national Supervisory Body, as soon as it becomes aware of it, of any bankruptcy proceedings against Camerfirma, as well as of any other circumstance that will prevent the activity of Camerfirma as TSP.
- It shall notify the national Supervisory Body of the termination of its activity as a TSP issuing qualified certificates and, if applicable, of the reliable party that it will transfer any obligations (see below), at least three months in advance.
- It shall notify affected customers (Subscribers and Subjects of affected active certificates) and other affected entities with which it has agreements or other types of relationships, of termination of activity at least two months in advance.
- It shall publish the relevant information concerning the termination of activity on its website or any other means accessible to Relying Parts, at least two months in advance.
- It shall revoke any authorization from subcontracted entities to act on behalf of Camerfirma in carrying out any functions relating to the process of issuing qualified certificates.
- It shall terminate any affected Camerfirma CA under this CPS (see section 5.8.2).
- It shall, with regard to the affected CAs, continue to carry out its obligations related to maintaining registration information and event log archives, and to providing information on revocation status of issued certificates, for the period of time indicated to Subscribers, Subjects, Persons Responsible and Relying Parties (15 years after the expiry of certificates), or it will transfer these obligations to a reliable party.

All these activities will be included in detail in the Camerfirma Termination Plan for Qualified Trust Services.

Before Camerfirma ceases its activity as a TSP issuing non-qualified certificates:

- 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 affected customers (Subscribers and Subjects of affected active end entity certificates, and/or Entities owning external Subordinate CAs with affected active certificates) and other affected entities with which it has agreements or other types of relationships, of termination of activity.
- It shall publish the relevant information concerning the termination of activity on its website or any other means accessible to Relying Parties.
- It shall revoke any authorization from subcontracted entities to act on behalf of Camerfirma in carrying out any functions relating to the process of issuing non-qualified certificates.
- It shall terminate any affected Camerfirma CA under this CPS (see section 5.8.2).
- It shall, with regard to the affected CAs, continue to carry out its obligations related to maintaining registration information and event log archives, and to providing information on the revocation status of issued certificates, for the period of time indicated to Subscribers, Subjects, Persons Responsible and Relying Parties (15 years after the expiry of certificates), or it will transfer these obligations to a reliable party.

In accordance with Law 6/2020, Camerfirma shall notify the national Supervisory Body of the termination of its activity as a TSP issuing non-qualified certificates and, if applicable, of the reliable party that it will transfer any obligations, within three months of termination of its activity.

5.8.2 TERMINATION OF A CA

Camerfirma shall terminate any CA under this CPS in case of compromise of its private key or for other reasons, such as, for example, the expiry of its certificate or the cessation of Camerfirma's activity as a TSP issuing qualified certificates and/or as a TSP issuing non-qualified certificates (see section 5.8.1).

Before Camerfirma terminates any CA under this CPS for compromise of its private key, in accordance with the provisions of section 5.7.3:

- If the CA is a Subordinate CA, it shall revoke its certificate/s associated with the compromised private key.
- It shall inform the national Supervisory Body, affected RAs, affected customers, Relying Parties and other affected entities with which it has agreements or other types of relationships.

Before Camerfirma terminates any CA under this CPS for a reason other than the compromise of its private key:

- If the CA has active end entity issued certificates, it shall notify its respective Subscribers, and Subjects of the termination of the CA and, in case the CA is replaced by a new CA or by another existing CA, it shall offer them the possibility of issuing new certificates with the other CA.

- If the CA has active external Subordinate CA certificates, it shall notify its respective owning Entities of the termination of the CA and, in case the CA is replaced by a new CA or by another existing CA, it shall offer them the possibility of issuing new certificates with the other CA.
- Where applicable, it will notify other affected entities with which it has agreements or other relationships of the termination of the CA.

Camerfirma shall terminate a CA under this CPS when the following actions have been completed:

- It shall stop issuing certificates by the CA.
- It shall revoke all active certificates issued by this CA.
- In case the CA is listed in the Trusted List (TSL) as a service issuing qualified certificates with current status *granted*, it shall apply to the national Supervisory Body for its status to be changed to *withdrawn*.
- After revoking all active certificates issued by the CA, it shall issue and publish the CA's last CRL/s, which will include the revoked certificates that have expired and will be valid until 31/12/9999 UTC time.

In case of compromise of the CA's private key, the last CRL/s shall be signed with a new private key associated with a new CA certificate, in accordance with the provisions of section 5.7.3.

- If there is no compromise of the CA's private key, the CA's OCSP service shall no longer provide information on the status of certificates issued by the CA (the service's responses shall contain the status *unknown* and shall be signed with a *default* OCSP certificate; see section 1.3.1.5).

In case of compromise of the CA's private key, the OCSP service shall continue to provide information on the status of certificates issued by the CA at the same access address, with responses signed with a *default* OCSP certificate (see section 1.3.1.5).

- After issuing of the last CRL/s, if the CA is a Subordinate CA, its certificate/s shall be revoked by the corresponding issuing CA or shall expire.

In case of compromise of the CA's private key, its new certificate associated with the new private key used to sign the last CRL(s) shall be revoked (its certificate/s associated with the CA's compromised private key shall have already been revoked previously, in accordance with the provisions of section 5.7.3).

- After issuing the last CRL/s, it shall destroy the CA's private key, including all backup copies identified by Camerfirma, in a manner such that the private key cannot be retrieved, and in accordance with a previously established procedure.

In case of compromise of the CA's private key, the CA's new private key associated with the new CA certificate shall also be destroyed in the same way.

- Where appropriate, 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.

Camerfirma shall consider any external Subordinate CA within the hierarchies under this CPS as terminated when its certificate(s) is/are revoked by the corresponding issuing CA.

Once a CA is terminated, it shall not be included in the next versions of these CPS and CPs. The corresponding change shall be indicated in the document history of the version in which the CA is removed.

Camerfirma shall consider one of the CPs in this document as terminated when there are no active certificates issued under that CP by the corresponding issuing CA/s.

Once a CP is terminated, it shall not be included in the next versions of these CPS and CPs. The corresponding change shall be indicated in the document history of the version in which the CP is removed.

5.8.3 TERMINATION OF A RA

In the event of termination of a RA:

- The CA shall stop issuing certificates through the RA.
- The CA shall revoke all active certificates issued through the RA, unless there is an agreement between the CA and the RA to keep them active.
- The RA shall deliver to the CA the information and documentation that has been necessary for the issuance and management of the certificates through the RA.
- The RA shall provide the CA with all existing information about ongoing and not yet validated certificate applications, so that the CA can validate them once compliance with the requirements of the corresponding applicable CPs has been verified.
- The RA shall guarantee that it will maintain, indefinitely, the confidentiality to which it has been obliged by virtue of the contract with the CA.

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 FIPS 140-2 level 3 or CC EAL 4 or higher.

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

The creation of Subordinate CAs keys is generated in HSM equipment certified FIPS 140-2 level 3 or CC EAL 4 or higher, 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	Expiry
CHAMBERS OF COMMERCE ROOT – 2016	4096 bits	sha256WithRSAEncryption	14/04/2016	08/04/2040
AC CAMERFIRMA FOR NATURAL PERSONS - 2016	4096 bits	sha256WithRSAEncryption	14/04/2016	09/03/2040
AC CAMERFIRMA FOR LEGAL PERSONS - 2016	4096 bits	sha256WithRSAEncryption	14/04/2016	09/03/2040
AC CAMERFIRMA TSA – 2016	4096 bits	sha256WithRSAEncryption	14/04/2016	09/03/2040
Chambers of Commerce Root – 2008 (certificate SHA-1)	4096 bits	sha1WithRSAEncryption	01/08/2008	31/07/2038
Chambers of Commerce Root – 2008 (certificate SHA-256)	4096 bits	sha256WithRSAEncryption	07/12/2011	31/07/2038
Camerfirma TSA II – 2014	4096 bits	sha256WithRSAEncryption	16/12/2014	15/12/2037
Camerfirma Codesign II – 2014	4096 bits	sha256WithRSAEncryption	16/12/2014	15/12/2037
Camerfirma Corporate Sever II - 2015	4096 bits	sha256WithRSAEncryption	15/01/2015	15/12/2037
Camerfirma AAPP II – 2014	4096 bits	sha256WithRSAEncryption	16/12/2014	15/12/2037

GLOBAL CHAMBERSIGN ROOT – 2016	4096 bits	sha256WithRSAEncryption	14/04/2016	08/04/2040
AC CAMERFIRMA COLOMBIA – 2016	4096 bits	sha256WithRSAEncryption	14/04/2016	09/03/2040
CAMERFIRMA COLOMBIA SAS CERTIFICADOS – 001	4096 bits	sha256WithRSAEncryption	12/11/2019	04/11/2031
CAMERFIRMA COLOMBIA SAS CERTIFICADOS – 002	4096 bits	sha256WithRSAEncryption	12/11/2019	04/11/2031
AC CAMERFIRMA PERÚ – 2016	4096 bits	sha256WithRSAEncryption	11/10/2016	10/03/2040
AC CAMERFIRMA PERÚ CERTIFICADOS – 2016	4096 bits	sha256WithRSAEncryption	11/10/2016	09/02/2040
CAMERFIRMA ROOT 2021	4096 bits	sha384WithRSAEncryption	19/10/2021	13/10/2045
AC CAMERFIRMA QUALIFIED CERTIFICATES - 2021	4096 bits	sha384WithRSAEncryption	20/10/2021	16/10/2037
INFOCERT-CAMERFIRMA CERTIFICATES 2024	384 bits	sha384ECDSA	22/01/2024	22/01/2045
INFOCERT-CAMERFIRMA QUALIFIED CERTIFICATES - 2024	384 bits	sha384ECDSA	16/02/2024	16/02/2040
INFOCERT-CAMERFIRMA TIMESTAMP 2024	384 bits	sha384ECDSA	22/01/2024	22/01/2045
INFOCERT- CAMERFIRMA QUALIFIED TSA - 2024	384 bits	Sha384ECDSA	16/02/2024	16/02/2040

6.1.1.1 CREATING THE SUBJECT'S KEY PAIR

Subjects can create their own keys using Camerfirma authorized SmartCard/Token devices or software devices authorized by Camerfirma, or RAs can create them using Camerfirma authorized SmartCard/Token devices, 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 certificate management platforms use their 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 Subject certificate. The certificate is delivered to the Person

Responsible 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 or ECDSA 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 certificate.
- 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 (RSA) or 256 bits (ECDSA).

6.1.1.2 KEY CREATION HARDWARE/SOFTWARE

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

The CAs keys use a cryptographic device that complies with FIPS 140-2 level 3 or CC EAL 4 or higher 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

See section 2.2.3.

6.1.5 KEY SIZES

The keys of CA certificates for active Root and Subordinate CAs within the hierarchies under this CPS are based on the RSA or ECDSA algorithm, with a length of 4096 bits (RSA) or 384 bits (ECDSA). See section 6.1.1.

The keys of end entity certificates under these CPS and CPs are based on the RSA or ECDSA algorithm with a minimum length of 2048 bits (RSA) or 256 bits (ECDSA).

6.1.6 PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING

The public key of CA certificates for active Root and Subordinate CAs within the hierarchies under this CPS and the public key of end entity certificates under these CPS and CPs are encrypted pursuant to IETF RFC 5280 and PKCS #1 standards. RSA or ECDSA are the key generation algorithm.

- Key creation algorithm: rsagen1 / ECDSA.
- Padding scheme: emsa-pkcs1-v1_5 / ECDSA.
- Hash functions: SHA-1 (only in CA certificates for Root CAs issued in 2008), SHA-256, SHA-384, 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* extensions, as defined in IETF RFC 5280 standard. More information is available in sections 4.1.5 and 7.1.2.

The private keys of Root CAs must not be used to sign end entity certificates, but only to sign the following cases:

- Root CA self-signed certificates.
- Certificates of Subordinate CAs under this CPS and external Subordinate CAs.
- OCSP certificates.

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 is generated and stored in HSMs that comply with FIPS 140-2 level 3 or CC EAL 4 or higher specifications and that are managed by at least two operators in a model n of m. The HSM are housed in secure environments.

The HSMs that store the Root CAs keys are managed inside an isolated and disconnected cryptographic room. The HSMs that store the Subordinate CA keys are hosted in secure environments within a CPD following ISO27001 regulations.

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

A backup is made of the CA private key which is stored and only retrieved by authorized 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 HSMs that comply with FIPS 140-2 Level 3 or CC EAL 4 or higher specifications.

6.2.1.2 THE SUBJECT'S PRIVATE KEY

The Subject's private key can be generated and stored in a software (PKCS #12), SmartCard/Token, centralized platform, HSM (TSU or CA certificate) or external device (PKCS #10).

In software (PKCS #12), Camerfirma provides configuration instructions for secure use.

In QSCD SmartCard/Token, keys are generated and stored in a device cryptographic smartcard/token QSCD, that complies with the requirements set out in Annex II of the eIDAS Regulation, and therefore are suitable for generating qualified electronic signatures and qualified electronic seals.

In SmartCard/Token (Non-QSCD or QSCD smartcard/token), keys are generated and stored in a device cryptographic smartcard/token FIPS 140-2 level 3 or CC EAL 4 or higher, Non-QSCD or QSCD.

In QSCD Cloud (QSCD centralized platform), keys are generated and stored in an HSM QSCD, which allows the Subject/Signatory (or Subject / Creator of a 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), and that complies with the requirements set out in Annex II of the eIDAS Regulation, and therefore are suitable for generating qualified electronic signatures and qualified electronic seals.

In Cloud (Non-QSCD or QSCD centralized platform), keys are generated and stored in an HSM FIPS 140-2 level 3 or CC EAL 4 or higher, Non-QSCD or QSCD, which allows the Subject/Signatory (or Subject / Creator of a 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 QSCD HSM (TSU certificate) keys are generated and stored in an HSM QSCD, that complies with the requirements set out in Annex II of the eIDAS Regulation, and therefore are suitable for generating qualified electronic seals.

In QSCD HSM (TSU or CA certificate), keys are generated and stored in an HSM FIPS 140-2 level 3 or FIPS 140-3 level 3 or CC EAL 4 or higher, Non-QSCD or QSCD.

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

Information regarding the key creation and custody process that Camerfirma uses is included in the 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.

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 centralized platform, QSCD or Non-QSCD, 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 Subject'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 Subject's keys created on SmartCard/Token cannot be copied because they cannot be taken out of the cryptographic device.

In a centralized platform, QSCD or Non-QSCD, the Subject's keys can be backed up under the terms established by the corresponding regulations.

Camerfirma keeps records on CA private key management processes.

6.2.5 PRIVATE KEY ARCHIVAL

CA private keys are not archived after termination of the CA because they are destroyed (see section 5.8.2).

Subjects 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.

Subjects 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 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.

Subjects' keys created on the software are created in Camerfirma's systems and are delivered to the Subject in a PKCS #12 software device.

Subjects' keys created on SmartCard/Token are created inside the cryptographic device delivered by the CA.

In a centralized platform, QSCD or Non-QSCD, 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 Subordinate 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 platform, QSCD or Non-QSCD, as stated in the description in the device manufacturer's manual.

6.2.8 METHOD OF ACTIVATING PRIVATE KEY

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

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

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

In a centralized platform, QSCD or Non-QSCD, 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.

6.2.9 METHOD OF DEACTIVATING PRIVATE KEY

For certificates on a SmartCard/Token, the Subject'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 platform, QSCD or Non-QSCD, 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, the certificate associated with them will be revoked.

The CA's private key shall be securely deleted from the cryptographic devices (HSMs) where it is stored, following the steps described in the HSM administration manual. Finally, all backup copies of the private key shall be securely deleted.

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

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

In a centralized platform, QSCD or Non-QSCD, 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

As stipulated in section 6.2.1 of this document.

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 certificate to retrieve the encrypted data.

All certificates issued by Camerfirma are valid from the moment of signature until the expiration date.

The periods of validity of certificates under this CPS and CPs are:

- Active Root and Subordinate CA certificates within the hierarchies under this CPS: see section 6.1.1.
- OCSP certificates (see section 1.3.1.5): 1 year.
- Qualified certificates issued by Camerfirma Subordinate CAs: not more than 5 years.
- Non-qualified certificates issued by Camerfirma Subordinate CAs: not more than 6 years.

6.4 ACTIVATION DATA

6.4.1 ACTIVATION DATA GENERATION AND INSTALLATION

The activation data of the Subject'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 Person Responsible via the email address associated with the 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 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 a centralized platform, QSCD or Non-QSCD, the keys are generated in an 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 Subject of the associated certificate. The platform allows the activation of 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 for certificates in software or SmartCard/Token format. Camerfirma do not store them for certificates in the centralized platform, as they are known and kept by the Subject. 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 Subject has not made a change in them previously.

In a centralized platform, QSCD or Non-QSCD, as described in the description in the manufacturer's manual of the device delivered to the Subject 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 Subject'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

As regards SmartCard/Token devices:

- 1) QSCD SmartCard/Token devices are certified QSCD. Non-QSCD or QSCD smartcard/token devices are certified FIPS 140-2 level 3 or CC EAL 4 or higher.
- 2) SmartCard/Token devices are prepared and sealed by an external provider.
- 3) The external provider sends the device to the registration authorities to be delivered to the Subject.
- 4) The Subject or RA uses the device to generate the key pair and send the public key to the CA.
- 5) The CA sends a public key certificate to the Subject or RA, which is entered into the device.
- 6) The device can be reused and can store several key pairs securely.
- 7) The device is owned by the Subject.

With respect to the centralized platform devices:

- QSCD Cloud devices use an HSM to store the keys certified and QSCD, and are authorized by the Supervisory Body for services catalogued as QSCDManagedOnBehalf.
- Non-QSCD or QSCD centralized platform devices use an HSM to store the keys certified

FIPS 140-2 level 3 or CC EAL 4 or higher.

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 measures taken for acceptance, implementation or rejection of the change are documented in the RFC.

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.

6.6.2 SECURITY MANAGEMENT CONTROLS

6.6.2.1 SECURITY MANAGEMENT

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

An annual training plan has been established for such purposes.

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

6.6.2.2 DATA AND ASSET CLASSIFICATION AND MANAGEMENT

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

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

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

6.6.2.3 MANAGEMENT PROCEDURES

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

process in detail.

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

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.

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.

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.

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.

6.6.2.8 ACCESS SYSTEM MANAGEMENT

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

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 authorized 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 authorized 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.

6.8 TIME-STAMPING

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

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

Certificate profiles under these CPS and CPs comply with IETF RFC 5280 and ITU-T X.509 standards and the applicable ETSI EN 319 412 standards.

Qualified certificates profiles under these CPS and CPs comply with IETF RFC 3739 standard and the applicable ETSI EN 319 412 standards.

Camerfirma publishes the datasheets of certificate profiles under these CPS and CPs on the website <https://www.camerfirma.com/practicas-de-certificacion-ac-camerfirma-cps-dpc/>.

7.1.1 VERSION NUMBER

All certificates are X.509 version 3.

7.1.2 CERTIFICATE EXTENSIONS

Certificate extensions are described in the certificate profiles datasheets (see section 7.1).

7.1.3 ALGORITHM OBJECT IDENTIFIERS

The signature algorithm OID can be:

- 1.2.840.113549.1.1.5 - sha1WithRSAEncryption (only in CA certificates for Root CAs issued in 2008)
- 1.2.840.113549.1.1.11 – sha256WithRSAEncryption
- 1.2.840.113549.1.1.12 - sha384WithRSAEncryption
- 1.2.840.113549.1.1.13 – sha512WithRSAEncryption
- 1.2.840.10045.4.3.2 – sha256WithECDSAEncryption
- 1.2.840.10045.4.3.3 – sha384WithECDSAEncryption

The public key algorithm OID in *Subject Public Key Info* field is:

- 1.2.840.113549.1.1.1 - *rsaEncryption*
- 1.2.840.10045.2.1 - *ECC*

Algorithm OIDs are specified in the certificate profiles datasheets (see section 7.1).

7.1.4 NAME FORMS

Certificates contain the Subject's data (names) that is required for its use in the *Subject* field and, if applicable, in the *Subject Alternative Name* extension, in accordance with the provisions of these CPS and CPs.

In general, certificates for use in the public sector must include the following Subject's data in the *Subject* field and, if applicable, in the *Subject Alternative Name* extension:

- Where applicable, name and surname of the natural person Subject, in separate fields, or indicating the algorithm that allows its separation automatically.
- Where applicable, full registered name of the Entity (legal person or non-legal entity).
- Identification documents numbers of the natural person Subject and/or the Entity, in accordance with the applicable law.

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

The forms and semantics of the data included in the *Subject* field and, if applicable, in the *Subject Alternative Name* extension are described in the certificate profiles datasheets (see section 7.1).

7.1.5 NAME CONSTRAINTS

Camerfirma may define name restrictions (see section 7.1.4) in external Subordinate CA certificates, through the *Name Constraints* extension, so that these CAs can only issue of certificates with names that comply with the restrictions defined in this extension.

7.1.6 CERTIFICATE POLICY OBJECT IDENTIFIER

End entity certificates contain a CP OID that starts from the base 1.3.6.1.4.1.17326, which identifies the applicable Camerfirma PC.

End entity certificates may contain the applicable CP OIDs defined in national regulations, and/or in ETSI standards, and/or in other applicable regulations.

CA certificates, in general, contain the CP OID 2.5.29.32.0 (*anyPolicy*), but, in some cases, may contain other OID/s.

CP OIDs contained in certificates are specified in the certificate profiles datasheets (see section 7.1), and in sections 1.2, 1.3.1.1, 1.3.1.2 and 1.3.1.3.

7.1.7 USAGE OF POLICY CONSTRAINTS EXTENSION

Camerfirma may define policy restrictions in external Subordinate CA certificates, through the *Policy Constraints* extension, so that these CAs can only issue of certificates with policies that comply with the restrictions defined in this extension.

7.1.8 POLICY QUALIFIERS SYNTAX AND SEMANTICS

Certificates may contain policy qualifiers *CPS Pointer* and/or *User Notice* with the syntax and semantics specified in the IETF RFC 5280 standard.

Policy qualifiers OIDs contained in certificates are specified in the certificate profiles datasheets (see section 7.1).

7.1.9 PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICIES EXTENSION

The *Certificate Policies* extension is not marked as “critical” in the certificates, in any case.

7.2 CRL PROFILE

CRL profiles issued by CAs under this CPS comply with IETF RFC 5280 and ITU-T X.509 standards.

The CRLs are signed by the same CA that signs the certificates, using the same private key.

The validity period of the CRLs for each CA is specified in section 4.9.7.

7.2.1 VERSION NUMBER

All CRLs are X.509 version 2.

7.2.2 CRL AND CRL ENTRY EXTENSIONS

All CRLs include the following CRL extensions:

- *CRL Number* (OID 2.5.29.20), non-critical, as defined in IETF RFC 5280 standard.
- *Authority Key Identifier* (OID 2.5.29.35), non-critical, as defined in IETF RFC 5280 standard.

CRLs may include the following CRL extensions:

- *ExpiredCertsOnCRL* (OID 2.5.29.60), non-critical, as defined in ITU-T X.509 standard, with the date and time value in the *Validity notBefore* field of the CA certificate.
- *Issuing Distribution Point* (OID 2.5.29), critical, as defined in IETF RFC 5280 standard.

CRLs include the following CRL entry extension:

- *Reason Code* (OID 2.5.29.21), non-critical, as defined in IETF RFC 5280 standard.

7.3 OCSP PROFILE

OCSP responses profiles complies with IETF RFC 6960.

The OCSP responses include the reason for revocation within the information of each revoked certificate.

The validity period of OCSP responses for each CA is specified in section 4.9.10.

The OCSP certificate profile complies with section 7.1.

7.3.1 VERSION NUMBER

The version of OCSP responses is v1, in accordance with IETF RFC 6960 standard.

7.3.2 OCSP EXTENSIONS

OCSP responses include the following extensions:

- *Nonce* (OID 1.3.6.1.5.5.7.48.1.2), non-critical, as defined in IETF RFC 6960 standard.
- *Archive CutOff* (OID 1.3.6.1.5.5.7.48.1.6), non-critical, as defined in IETF RFC 6960 standard, with the date and time value in the *Validity notBefore* field of the CA certificate.
- *Extended Revoked Definition* (OID 1.3.6.1.5.5.7.48.1.9), non-critical, as defined in IETF RFC 6960 standard.

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, ISO 22301, ISO 14001 and ENS 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.

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.

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

Camerfirma periodically performs the necessary audits, as detailed bellow:

- ISO 27001, ISO 20000, ISO 9001, ISO 22301 and ISO 14001 auditing on a three-year cycle with annual reviews.
- Spanish National Security Scheme (ENS), biennial.
- 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 analysis quarterly.
- Penetration test yearly.
- RA audits on a discretionary basis.

8.1.1 EXTERNAL SUBORDINATE CA AUDITS OR CROSS-CERTIFICATION

Not applicable.

8.1.2 AUDITING THE RAS

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.

The audit process is carried out by sampling the certificates issued and verifying that they have been issued in accordance with Camerfirma's CP.

8.1.3 SELF-AUDITS

Annually Camerfirma performs internal audits off all the standards indicated in point 8.1 (technical and legal control).

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

The audits are carried out by the following external and independent companies. They are widely recognised in IT security, information systems security and Certification Authorities compliance audits:

- For ISO 27001, ISO 20000, ISO 9001, ISO 22301 audits - CSQA. <https://www.csqa.it>
- For ISO 14001 and ENS audit - CAMARA CERTIFICA. <https://www.camaracertifica.es>
- For conformity assessment of eIDAS Natural Persons & Legal Persons - CSQA. <https://www.csqa.it>
- For conformity assessment of eIDAS Timestamps - CSQA. <https://www.csqa.it>
- For internal audits and Personal Data Protection Act - AUREN <https://www.auren.com>

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The assessments bodies are independent and reputed companies with specialist IT audit departments that manage certificates and trust 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 the assessments bodies and Camerfirma.

8.4 TOPICS COVERED BY ASSESSMENT

In general terms, the audits verify:

- Camerfirma has a system that guarantees service quality.
- Camerfirma complies with the requirements of the CPs that regulate the issuance of the different types of certificates.
- Camerfirma properly manages the security of its information systems.

In general, the elements audited are:

- Camerfirma, AR processes and elements related to the issuance of certificates, time stamps and online validation services (OCSP).
- Information security systems.
- Physical and logical protection of data processing centres.
- Documentation required for the issuance of each type of certificate.
- Verification that RA operators are aware of and comply with the CPD and CPs.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

Once the compliance audit assessment report has been received, Camerfirma shall review the deficiencies found with the entity that performed the audit and shall develop and execute a corrective action plan to resolve the deficiencies.

If the audited entity is unable to develop and/or execute said plan within the requested timeframe, or if the deficiencies found pose an immediate threat to the security or integrity of the system, it must immediately notify the policy authority, which may execute 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 91 136 91 05.

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

9.1.2 CERTIFICATE ACCESS FEES

Access to certificates is free-of-charge, although 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 91 136 91 05.

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 CRLs.

Camerfirma provides the OCSP service free-of-charge.

9.1.4 FEES FOR OTHER SERVICES

Access to the content of these CPS and CPs is free-of-charge on Camerfirma's website <https://www.camerfirma.com/practicas-de-certificacion-ac-camerfirma-cps-dpc/>.

9.1.5 REFUND POLICY

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

The correct issuance of the 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).

9.2 FINANCIAL RESPONSIBILITY

9.2.1 INSURANCE COVERAGE

Camerfirma, in its role as a TSP, has a public liability insurance policy that covers its liabilities to pay compensation for damages and losses caused to the users of its services: the Subject/Signatory and the 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.

9.3.2 INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION

Camerfirma considers the following information not confidential:

- 1) The contents of these CPS and 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 certificates, the Subjects or the Persons Responsible 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 has online query services for the status of certificates based on the OCSP standard. The OCSP services provide standardized responses under IETF RFC 6960 about the status of a certificate, i.e. whether the queried certificate is active, revoked or whether it has been issued or not by the CA.

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

9.4.2 INFORMATION TREATED AS PRIVATE

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

9.4.3 INFORMATION NOT DEEMED PRIVATE

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

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 CA REPRESENTATIONS AND WARRANTIES

9.6.1.1 CAS UNDER THIS CPS

In accordance with the stipulations of these CPS and CPs, and in accordance with applicable regulations in force regarding certification service provision, Camerfirma, acting as a TSP issuing certificates (CAs under this CPS), shall be obliged to:

- Adhere to the provisions of these CPS and CPs and applicable regulations in force.
- Protect its private keys and keep them secure.
- Issue certificates in accordance with these CPS and CPs, and the applicable technical standards.
- Issue certificates in accordance with the information in its possession and which do not contain errors.
- Issue certificates with the content defined by current law for qualified certificates.
- Respect in any case the provisions on the protection of personal data in the regulations in force.
- Suspend and revoke certificates in accordance with these CPS and CPs and publish the revocations and suspensions in CRLs and OCSP services.
- Inform Subjects about the revocation or suspension of their certificates, on time and in accordance with current law.
- Publish current, past and new versions of these CPS and CPs on its website.
- Notify new versions of these CPS and CP to the Supervisory Body.
- Inform RAs about modifications to these CPS and CP that affect their functions.
- Do not store or copy the Subjects' private keys except for encryption certificates and when it is legally provided for or allowed to be stored or copied.
- If the CA (or, when applicable, another QTSP or TSP) generates the Subject's keys, generate (or, when applicable, confirm that another QTSP or TSP generates) the keys using an algorithm recognized as acceptable for the use of the certificate and the private key, including, where applicable, the advanced or qualified electronic signature, or the advanced or qualified electronic seal, during the period of validity of the certificate, and in accordance with the requirements of the corresponding CP.
- If the CA (or, when applicable, another QTSP or TSP) generates the Subject's keys, use (or, when applicable, confirm that another QTSP or TSP uses) key lengths and algorithms recognized as acceptable for the use of the certificate and the private key, including, where applicable, the advanced or qualified electronic signature, or the advanced or qualified electronic seal, during the period of validity of the certificate, and in accordance with the requirements of the corresponding CP.
- If the CA generates the Subject's keys, protect the keys with due diligence while in its safekeeping.

- If the CA generates the Subject's keys, for certificates issued on secure cryptographic devices SmartCard/Token, QSCD or Non-QSCD, generate the keys within the secure cryptographic device SmartCard/Token, QSCD or Non-QSCD.
- For certificates issued on Cloud devices, QSCD or Non-QSCD, managed by the CA (or, when applicable, by another QTSP or TSP) generate within an HSM, QSCD or Non-QSCD, and keep (or, when applicable, confirm that another QTSP or TSP generates within an HSM, QSCD or Non-QSCD, and keeps) with due diligence the private keys of the certificates, ensuring that they can only be used within an HSM, QSCD or Non-QSCD, under the sole control of the Subjects/Signatories (or under the control of the Subjects / Creators of a Seal).
- Establish data creation and custody systems in the aforementioned activities, protecting data from being lost, destroyed or forged.
- Keep data relating to the issued certificate for the minimum period required by current law.

Camerfirma's responsibility:

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

Trust 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 provision of trust electronic services, including identity verification activities prior to the issuance of a qualified certificate.

- Article 13 of 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 or the Relying Party, and other third parties in accordance with the terms and conditions established under current law, the Terms and Conditions and these CPS and CPs.

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 Subject's details and the RA practices.
- Guaranteeing that when the certificate is delivered, the Subject is in possession of the private key relating to the public key contained in the certificate, when the certificate issuance process requires it, by using standard request in PKCS #10 format.
- Guaranteeing that the public and private keys work in conjunction with each other, using certified cryptographic devices and mechanisms.
- That the certificate requested and the certificate delivered match.
- Any liability established under current law.

In accordance with current law, Camerfirma holds a public liability insurance policy that fulfils the requirements established in these CPS and CPs.

9.6.1.2 EXTERNAL SUBORDINATE CAS

Not applicable.

9.6.2 RA REPRESENTATIONS AND WARRANTIES

RAs are entities that the CA appoints to register and approve certificates and, where applicable, processing requests for revocation and reports of events relating to revocation of certificates. Therefore, the RAs also carry out the obligations defined in these CPS and CPs for issuing certificates, particularly to:

- Adhere to the provisions of these CPS and CPs and applicable regulations in force.
- Protect their private keys that are used for exercising their functions.
- Check the identity of the Subscribers, the Applicants, the Persons Responsible, the Subjects and the Entities of certificates when necessary, definitively proving the identity of the Subject/Signatory, for individual certificates, or the Subject / Creator of a Seal, for organization certificates, in accordance with the provisions in this CPS and CPs.
- Check the accuracy and authenticity of information provided by the Applicant, and, where applicable, by the Person Responsible, and/or the Subscriber, and/or the Entity.
- Respect in any case the provisions on the protection of personal data in the regulations in force.
- Provide the Person Responsible and, if applicable, the Subject and/or the Subscriber access to the certificate.
- If applicable, deliver the corresponding cryptographic device to the Person Responsible.
- Archive the documents provided by the Applicant and/or, where applicable, by the Person

Responsible, and/or the Subscriber, and/or the Entity for the period required by current law.

- Respect contract provisions signed with Camerfirma and, if applicable, with the Subscriber an/or the Subject.
- Where applicable, process requests for revocation and reports of events relating to revocation.
- Where applicable, inform the CA about the causes for revocation, when known.
- Provide basic information about the certificate's policy and use, especially including information about the CA and the applicable CPS and CP, as well as their obligations, powers and responsibilities.
- Provide information about the certificate and, if applicable, the cryptographic device.
- Compile information and evidence from the Person Responsible for the receipt of the certificate and, if applicable, the cryptographic device, and acceptance of such elements.
- Inform the Subject/Signatory of the use under its sole control (and the Subject / Creator of a Seal of the use under its control) of the certificate's private key and its activation data, according to these CPS and CPs.
- If the RA generates the Subject's keys, generate the keys using an algorithm recognized as acceptable for the use of the certificate and the private key, including, where applicable, the advanced or qualified electronic signature, or the advanced or qualified electronic seal, during the period of validity of the certificate, and in accordance with the requirements of the corresponding CP.
- If the RA generates the Subject's keys, use key lengths and algorithms recognized as acceptable for the use of the certificate and the private key, including, where applicable, the advanced or qualified electronic signature, or the advanced or qualified electronic seal, during the period of validity of the certificate, and in accordance with the requirements of the corresponding CP.
- If the RA generates the Subject's keys, protect the keys with due diligence while in its safekeeping.
- If the RA generates the Subject's keys, for certificates issued on secure cryptographic devices SmartCard/Token, QSCD or Non-QSCD, generate the keys within the secure cryptographic device SmartCard/Token, QSCD or Non-QSCD.
- If applicable, for certificates issued on Cloud devices, QSCD or Non-QSCD, managed by the RA generate within an HSM, QSCD or Non-QSCD, and keep with due diligence the private keys of the certificates, ensuring that they can only be used within an HSM, QSCD or Non-QSCD, under the sole control of the Subjects/Signatories (or under the control of the Subjects / Creators of a Seal).

These obligations are even in cases of entities delegated by the RAs such as Points of Physical Verification (PPV) and Points of Remote Verification (PRV), where applicable.

The information about the use and responsibilities of the Subject and, where applicable, of the Responsible is provided once the terms of use are accepted prior to the confirmation of the certificate application and via email.

RAs' responsibility:

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

1) Obligations prior to issuing a certificate.

- Informing Subscribers, Applicants and Persons Responsible about the acceptance of their obligations and responsibilities.
- Properly identifying Applicants, who must be persons entitled to apply for the certificate.
- Checking the validity of the Applicant's details and, if there is a relationship or powers of representation, the Entity's and/or Subject details.
- Where applicable, properly identifying Subscribers and/or Persons Responsible.
- Accessing the RA application to manage requests.

2) Obligations once the certificate has been issued.

- Managing certificates while they are still in force (expiry, suspension, revocation).
- Archiving copies of submitted documentation and, if applicable, the signed agreements, in accordance with the CPS and CPs published by the CA and current law.

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

In the event of a claim from a Subscriber, a Subject, an Entity or a Relying Party, 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 a Subscriber, a Subject, an Entity or a Relying Party, and this 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 the CA in the event of breach.

Of course, it is not CA'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 the CA, not only based on controls of files and procedures for preservation of files received by the RA, 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 (PPV) and Points of Remote Verification (PRV), without prejudice to their right to contest them.

9.6.3 SUBSCRIBER REPRESENTATIONS AND WARRANTIES

9.6.3.1 SUBSCRIBER

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

- Accept the Terms and Conditions imposed by the CA.
- Where applicable, provide the RA with the necessary information and/or documentation to carry out its correct identification.
- Where applicable, provide the RA with required information and/or documentation of the Subject and/or the Entity.
- Where applicable, provide the RA with required information and/or documentation of the Applicant and/or the Person Responsible, in accordance with provisions on the protection of personal data in the regulations in force.
- Where applicable, guarantee the accuracy and veracity of the information and/or the documentation provided.
- Where applicable, inform the RA or the CA of any change in the data provided for the issuance of the certificate and contained in it, during the period of validity of the certificate.
- Request to the RA or the CA as soon as possible the revocation of the certificate when it becomes aware of the existence of any cause for revocation.
- Where applicable, respect the provisions of the documents signed with the CA and/or the RA.

9.6.3.2 APPLICANT

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

- Provide the RA with the necessary information and/or documentation to carry out his/her correct identification, in accordance with provisions on the protection of personal data in the regulations in force.
- Where applicable, provide the RA with required information and/or documentation of the Subject and/or the Entity.
- Where applicable, provide the RA with required information and/or documentation of the Applicant and/or the Person Responsible, in accordance with provisions on the protection of personal data in the regulations in force.

- Guarantee the accuracy and veracity of the information and/or the documentation provided.
- Where applicable, inform the RA or the CA of any change in the data provided for the issuance of the certificate and contained in it, during the period of validity of the certificate.
- Inform the RA or the CA as soon as possible of the existence of any cause of revocation.

9.6.3.3 SUBJECT AND PERSON RESPONSIBLE

The Subject, and the Person Responsible if different than the Subject, of a certificate shall be obliged to comply with the provisions of the applicable regulations in force and in addition to:

- Accept the Terms and Conditions imposed by the CA.
- Responsible: where applicable, provide the RA with the necessary information and/or the documentation to carry out a correct identification, in accordance with provisions on the protection of personal data in the regulations in force.
- Responsible: where applicable, provide the RA with required information and/or documentation of the Subject and/or the Entity.
- Responsible: where applicable, provide the RA with required information and/or documentation of the Applicant and/or the Person Responsible, in accordance with provisions on the protection of personal data in the regulations in force.
- Responsible: where applicable, guarantee the accuracy and veracity of the information and/or the documentation provided.
- Responsible: where applicable, inform the RA or the CA of any change in the data provided for the issuance of the certificate and contained in it, during the period of validity of the certificate.
- Request to the RA or the CA as soon as possible the revocation of the certificate when it becomes aware of the existence of any cause for revocation.
- Where applicable, respect the provisions of the documents signed with the CA and/or the RA.
- Use the certificate as established in the CPS and CPs in force.
- Not to use the private key neither the certificate from the moment in which it is requested or it is warned by the CA or the RA of the suspension or revocation of the certificate, or once the term of validity of the certificate has expired.
- Make use of the 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. It may be held liable to Relying Parties and, where applicable, to the Entity he/she represents in case of not having

authorization, for the consequences that improper use or improperly controlled use may generate.

- Subject/Signatory: authorize the CA and the RA to proceed to the treatment of the personal data contained in the certificates, in accordance with provisions regarding data protection, 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 in the certificate is accurate, complete for the purpose of the certificate and is updated at all times.
- Inform immediately the RA or the CA of any inaccuracies in the certificate detected once it has been issued.
- For certificates issued on secure cryptographic devices, QSCD or Non-QSCD, use the private key within the secure cryptographic device, QSCD or Non-QSCD.
- Be especially diligent in the safekeeping of the private key and, if applicable, of the SmartCard/Token device, QSCD or Non-QSCD, in order to avoid unauthorized use.
- In the case of certificates in SmartCard/Token device, QSCD or Non-QSCD, in the event that it loses its possession, make it known to the RA or the CA as soon as possible and, in any case, within 24 hours following the production of the aforementioned circumstance, regardless of the specific event that originated it or the actions that it may eventually exercise.
- Not to use the private key, the certificate or any other technical support given by the CA or RA to carry out any transaction prohibited by the applicable law.

If the Subject or the Person Responsible generates the Subject's keys, when the certificate issuance process requires it, the Subject and, if applicable, the Person Responsible shall be obliged to:

- Generate the keys using an algorithm recognized as acceptable for the use of the certificate and the private key, including, where applicable, the advanced or qualified electronic signature, or the advanced or qualified electronic seal, during the period of validity of the certificate, and in accordance with the requirements of the corresponding CP.
- Use key lengths and algorithms recognized as acceptable for the use of the certificate and the private key, including, where applicable, the advanced or qualified electronic signature, or the advanced or qualified electronic seal, during the period of validity of the certificate, and in accordance with the requirements of the corresponding CP.
- For certificates issued on secure cryptographic devices, QSCD or Non-QSCD, generate the keys within the secure cryptographic device, QSCD or Non-QSCD.
- For certificates issued to natural persons, maintain the private key under the Subject/Signatory's sole control.
- For certificates issued to legal persons, maintain the private key under the Subject / Creator of a Seal's control.

- Person Responsible: deliver the public key to RA, by using standard request in PKCS #10 format.

9.6.3.4 ENTITY

In the case of those certificates that imply the association with an Entity, the Entity shall be obliged to comply with the provisions of the applicable regulations in force and in addition to:

- Where applicable, provide the RA with required information and/or documentation of the Subject and/or the Entity.
- Where applicable, provide the RA with required information and/or documentation of the Applicant and/or the Responsible, in accordance with provisions on the protection of personal data in the regulations in force.
- Where applicable, guarantee the accuracy and veracity of the information and/or the documentation provided.
- Where applicable, inform the RA or the CA of any change in the data provided for the issuance of the certificate and contained in it, during the period of validity of the certificate.
- Request to the RA or the CA as soon as possible the revocation of the certificate when it becomes aware of the existence of any cause for revocation, especially when the Subject ceases to be associated with 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 applicable regulations in force and in addition:

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

9.6.5 REPRESENTATIONS AND WARRANTIES OF OTHER PARTICIPANTS

No stipulation.

9.7 DISCLAIMERS OF WARRANTIES

In accordance with current law, the responsibility assumed by the CA and the RA does not apply in cases in which certificate misuse is caused by actions attributable to the Subscriber, the Applicant, the Subject, the Person Responsible, the Entity and the Relying Party due to:

- Not having provided the right information, initially or later as a result of changes to the circumstances described in the certificate, when the CA or the RA has not been able to detect the inaccuracy of the data.
- Having acted negligently in terms of storing the private key and keeping it confidential.
- Not having requested the revocation of the certificate in the event of doubts raised over their storage or confidentiality.
- Having used the private key once the certificate has expired, or once the certificate has been revoked, or while the certificate has been suspended.
- Exceeding the limits established in the certificate.
- Actions attributable to the Relying Party, if this party acts negligently, that is, when it does not check or heed the restrictions established in the certificate in relation to allowed use and limited number of transactions, or when it does not consider the certificate's validity situation.
- Damages caused to the Subject, the Entity, or Relying Parties due to the inaccuracy of the data contained in the 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 and/or, if applicable, the Person Responsible 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 the control of the keys associated with your certificate.

The CAs 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 these CPS and CPs.
- Improper or fraudulent use of certificates, CRLs or OCSP responses.
- Use of the information contained in certificates, CRLs or OCSP responses.

- Damages caused during verification of the causes for revocation/suspension.
- Due to the content of messages or documents signed or encrypted digitally.
- Failure to retrieve encrypted documents with the Subject's public key.

9.8 LIMITATIONS OF LIABILITY

The monetary limit of the transaction value may be expressed in the end entity certificate by including the corresponding QCStatement in the *Qualified Certificate Statements* extension, in accordance with the provisions of ETSI EN 319 412-5 standard.

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 these CPS and 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. 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 these CPS and CPs do not require notification except that it directly affects the rights of the Subscribers or the Subjects, 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 these CPS and CPs can be changed without notice.

9.12.2.2 NOTIFICATION METHOD

Any proposed changes to these CPS and CPs are published immediately on Camerfirma's website <https://www.camerfirma.com/practicas-de-certificacion-ac-camerfirma-cps-dpc/>

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 these CPS and/or CPs. Especially the changes in this CPS will be notified to the national Supervisor Body.

9.12.2.3 PERIOD FOR COMMENTS

The affected Subscribers and Subjects 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 these CPS and CPs is obliged to fulfil the requirements established within current Spanish and European Union law in force at each time.

9.15 COMPLIANCE WITH APPLICABLE LAW

See section 9.14.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 ENTIRE AGREEMENT

Parties to these CPS and CPs assume in their entirety the content of this document.

9.16.2 ASSIGNMENT

Parties to these CPS and CPs may not assign any of their rights or obligations under these CPS and CPs or applicable agreements without the written consent of Camerfirma.

9.16.3 SEVERABILITY

Should individually provisions of these CPS and 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 these CPS and 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 these CPS and CPs does not eliminate Camerfirma's right to enforce the same provisions later or the right to enforce any other provision of these CPS and 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	<p>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)</p> <p>1.2.1.3 - OIDs corrections of EP certificates with PSEUDÓNIMO (point 1.3.11.3 after adaptation to structure RFC3647)</p> <p>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)</p> <p>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)</p> <p>1.5.5 - Incorporation of the figure of Delegate Agency for Camerfirma Perú (point 1.3.2 after adaptation to structure RFC3647)</p> <p>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)</p>
Mar 2018	V1.2.3	<p>1.5.5 RAs for SSL can't validate the domain. CA / B Forum. (point 1.3.2 after adaptation to structure RFC3647)</p> <p>2.5.3 Clarification free service OCSP. (point 9.1.3 after adaptation to structure RFC3647)</p> <p>2.1.5 user responsibility - TSL check (point 9.6.4 after adaptation to structure RFC3647)</p>
May 2018	V1.2.4	<p>1.3.3, 1.3.9 y 1.3.10 Clarifications concepts Subject / Holder and Signer / Creator of the seal.</p> <p>3.2.3.1 Other documents accepted to prove the link between the owner of the domain and the certificate holder.</p> <p>9.1.5 Political modification of withdrawals</p> <p>9.4 Update of the privacy clause of personal information according to RGPD</p> <p>9.7 Exemption of responsibility of the CA and AR in case of delegation</p>

		<p>of the certificate to a third party</p> <p>Adaptation of the structure of the CPD document based on RFC3647</p> <p>1.3.11.3 Incorporation of hierarchy CHAMBERS OF COMMERCE ROOT - 2018</p> <p>1.3.11.4 Incorporation of subordinated CA AC CAMERFIRMA GLOBAL TSA – 2018</p>
Jun 2018	V1.2.5	<p>Nomenclature correction from safe device to qualified device.</p> <p>Correction of URLs by changing Camerfirma website.</p> <p>Incorporation of CA CN = Camerfirma Corporate Server II - 2015 as qualified CA.</p> <p>3.2.1 Storage of keys generated by Camerfirma and stored remotely.</p> <p>3.2.3.2 Corrections.</p> <p>3.2.3.4 Eliminated 3.2.3.4 Considerations in the identification of users and linkage in the AAPP.</p> <p>3.3.2 Incorporation of additional explanatory text.</p> <p>4.1.2.5 Modification cross-certification.</p> <p>8.1.1 Correction requirements for organizations with certificates of Intermediate CA or Camerfirma cross-certification.</p> <p>8.2 Update eIDAS auditors.</p>
Jul 2018	V1.2.6	<p>1.3.11.4.1.4 qualifying TSU certificates validity's is 5 years maximum</p> <p>8.7 Self-Audit about 3% of the Server Certificates.</p> <p>9.12.2.2 Nacional supervisor body notification ES, PE, CO, MX</p> <p>Change of order, denomination and development in different points to meet RFC3647</p> <p>Point '9.12.1 Procedure for amendment' is developed</p>
Sep 2018	V1.2.7	<p>Change of order, denomination and development in different points to meet RFC3647</p> <p>Point '9.12.1 Procedure for amendment' is developed</p>
Sep 2018	V1.2.8	<p>3.2.5.1 Proof of relationship, the domain validation will be done by one of the methods accepted by CA/B Forum</p> <p>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.</p>
Sep 2018	V1.2.9	<p>minor changes to the document format</p>

		<p>3.2.5.1 Identification of the link. Explicit statement of the methods used.</p> <p>3.2.3 Incorporation of the control check procedure on the applicant's email account.</p> <p>4.2.1 Included are the AAC checks previously stated in 3.2.5.2.</p> <p>Hierarchy withdrawn CHAMBERS OF COMMERCE ROOT - 2018</p> <p>9.16.4 updated</p> <p>6.2.3 updated</p>
Feb 2019	V1.2.10	<p>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.</p> <p>1.3.2 Includes CHAMBERS OF COMMERCE ROOT 2018 hierarchy</p> <p>1.3.5.7.3.1 the 2016 hierarchy is replaced by the 2018 hierarchy</p> <p>1.3.5.7.3.5 AC CAMERFIRMA FOR NATURAL PERSONS. (Certificates for natural persons)</p> <p>1.4.1 Appropriate uses of certificates</p> <p>1.4.2 Prohibited and Unauthorized Uses of Certificates</p> <p>1.6.2 Definition of Remote Signature and Remote Seal</p> <p>2.2.1 Certification Policies and Practices.</p> <p>2.2.2 Terms and Conditions.</p> <p>3.1.3 Remove reference to policies.</p> <p>3.1.5.1 Issuance of several physical person certificates for the same holder.</p> <p>3.1.6 Recognition, authentication and function of trademarks and other distinctive signs</p> <p>3.2.1 Methods of testing private key ownership and reference to QSCD list.</p> <p>3.2.2.1 Identity</p> <p>3.2.3 Identification of an individual's identity.</p> <p>3.2.2.5 IP URL record</p> <p>3.4 Identification and authentication of a revocation request</p> <p>4.1.2.4 elimination reference policies</p>

	<p>4.1.2.5 Cross certification notes</p> <p>4.2.2 clarification delivery documentation and WS access</p> <p>4.2.3 Unspecified Sub-CA period</p> <p>4.3.1.3 Authenticated WS Requests.</p> <p>4.5.1 Use of the certificate and the subscriber's private key, including conditions of use for remote signature and remote seal.</p> <p>4.5.1 Includes CHAMBERS OF COMMERCE ROOT 2018 hierarchy</p> <p>4.6.1 No component certificate renewals.</p> <p>4.9.2 Remove reference to policies.</p> <p>4.9.5 Clarification revocation</p> <p>4.12.1 Incorporation of key custody in a centralized device.</p> <p>5.2.1 Remove policy reference</p> <p>5.3.1 Delete reference document</p> <p>5.5.1 Custody of events related to the centralized key management platform.</p> <p>5.7 Delete reference document</p> <p>5.7.4 Delete time reference</p> <p>6.1.1 Includes CHAMBERS OF COMMERCE ROOT 2018 hierarchy</p> <p>6.1.1.1 Include onbehalf treatment</p> <p>6.2.1.2 Error in reference document go to 6.2.1.1 - Include Onbehalf</p> <p>6.2.3 Include onbehalf treatment</p> <p>6.2.4 Include onbehalf treatment</p> <p>6.2.6 Include onbehalf treatment</p> <p>6.2.7 Include onbehalf treatment</p> <p>6.2.8 Include onbehalf treatment</p> <p>6.2.9 Include onbehalf treatment</p> <p>6.2.10 Include onbehalf treatment</p> <p>6.2.11 Include onbehalf treatment</p> <p>6.4 Activation of signature data on a centralized platform.</p> <p>6.4.2 Include onbehalf treatment</p> <p>6.6 Centralized platform life cycle management.</p> <p>9.6.4 The responsibility of the Signatory/Creator of the seal and of the</p>
--	---

		<p>Subject/Holder in case of delegation of the use of certificates to third parties is warned.</p> <p>9.6.5 Obligation and responsibility of third parties, the obligations of certificates of Representative of Legal Person are detailed</p> <p>9.6.1.1 Incorporation of CA responsibility for centrally stored keys.</p> <p>9.6.2 Obligation and responsibility of the RA</p> <p>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.</p> <p>9.7 Liability disclaimer</p> <p>9.12.2.2 Communication of changes to auditors</p>
Jan 2020	V1.2.11	<p>1.3.1 Incorporates corporate data of AC Camerfirma SA and its participation by InfoCert, S.p.A.</p> <p>1.3.2 Adding requirements for issuing certificates to non-residents in Spain and for authorization of external RAs that issue Secure Server certificates</p> <p>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</p> <p>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.</p> <p>1.3.5.7.3 Update of the CHAMBERS OF COMMERCE Hierarchy:</p> <ul style="list-style-type: none"> - 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”) <p>1.3.5.7.3.2 Clarify how keys are generated and stored</p> <p>1.3.5.7.3.5.2.1 Clarifications of the functionalities of the Qualified Legal Representative Certificates,</p> <p>1.3.5.7.4 Update of the GLOBAL CHAMBERSIGN ROOT Hierarchy - 2016:</p> <ul style="list-style-type: none"> - revocation of intermediate CA “AC CAMERFIRMA – 2016” and all its second level intermediate CAs

		<ul style="list-style-type: none"> - 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”) <p>2.3 CPS version periodicity is incorporated</p> <p>3.2.2.1 In identifying the entity for SSL EV certificates, the entity category must be checked according to CA / Browser Forum policies</p> <p>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</p> <p>4.5.1 The key usage table is updated with the current CAs</p> <p>4.9 Where to check expired and non-expired certificates is required and for how long in case of intermediate CA revocation</p> <p>4.9.1 Added 2 revocation causes aligned with Mozilla Root Store Policy</p> <p>4.9.7 The CRL emission frequency table is updated with the current CAs</p> <p>6.1.1 The table on key pair generation with current CAs is updated</p> <p>6.1.7 It is explicitly stated that root keys do not issue end-entity certificates (except for OCSP responders)</p> <p>6.2.11 Control of the qualification of devices and actions in case of loss</p> <p>8.1.3 Clarification frequency internal audits and volume for SSL</p>
May 2020	V1.2.12	<p>1.3.2 where is said “domain possession” change to “domain control”</p> <p>1.3.5.7.3 CHAMBER OF COMMERCE Hierarchy: incorporation of CHAMBERS OF COMMERCE ROOT and intermediate CA “AC CAMERFIRMA CERTIFICADOS CAMERALES”</p> <p>1.3.5.7.3.3 Removal of information about Codesign certificates (AC CAMERFIRMA CODESIGN – 2016 has been revoked)</p> <p>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)</p> <p>3.2.3 Authentication of individual identity: new writing to incorporate eIDAS and national methods of identification.</p>

		<p>3.2.5.1 Added reference about preservation of information and documentation of data issuance in paper or electronical means.</p> <p>Domain ownership evidence is removed.</p> <p>4.5.1 The key usage table is updated with the current CAs</p> <p>4.9.7 The CRL emission frequency table is updated with the current CAs</p> <p>5.2.1 It is specified that an RA Operator cannot issue a certificate to himself</p> <p>6.1.1 The table on key pair generation with current CAs is updated</p> <p>7.3 OCSP Message Profile Specifications Required</p> <p>8.1 References to WebTrust Audits are removed and the ETSI standards on which the eIDAS audit is based are detailed.</p> <p>8.2 The identification of audits and auditors is updated</p>
Jan 2021	V1.2.13	1.3.5.7.3 and 1.3.7.5.4 Incorporation of OIDs
Feb 2021	V1.2.14	<p>3.2.1.1 Registration Agencies incorporation.</p> <p>4.3.1.4 ETSI TS 119 431-2 signature policy incorporation.</p> <p>4.6.1 Change in the period of key use for a TSU certificate.</p> <p>5.4.3 Audit log retention period updated.</p>
Mar 2021	V1.2.15	<p>1.1 (and the rest of the document) the reference to Law 59/2003 is eliminated and reference to Law 6/2020 is added.</p> <p>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.</p> <p>1.3.3.5.7.7.3.4.4.2 Clarifications on the powers of the Representatives and how to accredit them.</p> <p>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.</p> <p>1.4.1 and 1.4.2 Clarifications on appropriate uses of the certificates and prohibited uses</p> <p>3.2.5.1 Addition of information on the 'Documentation' supporting the certificates of Self-Employed and Self-Employed Member of a Professional Association.</p> <p>3.3.1 Clarification in the wording of validation for certificate renewal and compliance with Law 6/2020</p>

		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 this CPS applies 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 Peru (INDECOPI) 1.3.5.4 The definition of the "Entity" role is added for electronic seal certificates.

	<p>1.3.5.5 Definitions of "Applicant" and "Subscriber" roles are added according to Peruvian regulations.</p> <p>1.3.5.6 The definition of the "Responsible" of the certificate is added according to Peruvian regulations.</p> <p>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.</p> <p>1.4.2 It is considered prohibited and unauthorized uses, the ones determined by Peruvian regulations.</p> <p>1.6.1 Acronyms for CE and RE are added according Peruvian terminology.</p> <p>1.6.2 Definitions of Certification Authority and Registration Authority are modified to incorporate Certification Entities and Registration Entities according to Peruvian terminology.</p> <p>2.1 and 2.2 Add links to services on the Camerfirma Perú website.</p> <p>3.1.1 The contact telephone number is modified and the reference to TSL certificates is eliminated.</p> <p>3.2.2.1 It is added that the CA of Peru may use the Commercial Registry of Panama to identify the entities.</p> <p>3.2.3 Reference is added to the identity documents of a national or resident individual in Peru.</p> <p>3.3 Conceptual and terminological clarification applicable to CA Peru regarding the "re-issuance" of certificates.</p> <p>4.5.1 New profiles are added in the certificate use box and the subscriber's private key.</p> <p>4.6.1 Specific circumstances of the reissues of certificates under the CA Peru are added, although it is indicated that the service is not currently available.</p> <p>4.6.7 Paragraph on TSL certificate is deleted.</p> <p>5.7.1 It is specified that certificates will not be issued while CA private key compromise persists.</p> <p>5.8 Actions are added in the event of CA or RA termination to include Peruvian requirements.</p> <p>8. Throughout the section, a reference is added to the audits that</p>
--	---

		<p>apply to services provided in Peru.</p> <p>9. It is specified where to find the rates and refund policy for the services provided in Peru.</p> <p>9.2.1 Modification of the amounts covered by the Insurance by Law 6/2020 and reference about subsidiaries services coverage.</p>
Nov 2021	V1.2.19	<p>1.3.5.2 The declaration of the national supervisory body within the Spanish State is updated.</p> <p>1.3.5.7.3 The root 'Chambers of Commerce Root - 2008' is included.</p> <p>1.3.5.5.7.3 Additional information about the devices where the keys are generated is incorporated.</p> <p>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).</p> <p>1.3.5.7.3 The Timestamp certificates issued by Camerfirma AAPP II - 2014 are removed from this table.</p> <p>1.3.3.5.7.7.3.1.1 A declaration is withdrawn and incorporated into point 1.3.5.7.3.</p> <p>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.</p> <p>3.2.1 Improvement in the information provided on the different methods of proof of private key possession.</p> <p>3.2.3 Clarifications related to the methods of identification and incorporation of the reference into the assisted process with pre-validation of documentation.</p> <p>3.3 Correction to the name of the CA.</p> <p>4.1.2.1 Correction of the PKCS used and extended declaration.</p> <p>4.3.1.4 Clarification of the OIDs embedded in the certificates is incorporated.</p> <p>4.9.11 Replacement of the referenced web page.</p> <p>4.12.1 Statement that they can be qualified and non-qualified devices.</p> <p>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'.</p> <p>6.1.1.1 Rewording of the paragraph referring to CKCs.</p> <p>6.2.1.2 More information is provided on generation in the centralized platform and the checks Camerfirma performs.</p>

		<p>6.2.3 The exception for keys generated in centralized platforms managed by Camerfirma is included.</p> <p>6.2.11 More information on generation in the centralized platform is added.</p> <p>9.12.2.2.2 Substitution of <i>Ministerio de Economía y Empresa</i> for National Supervisory Body.</p>
17/05/2022	V1.2.20	<p>The document format is updated and a document code is added.</p> <p>The possibility of generating keys on non-qualified devices (cards and tokens) is incorporated.</p> <p>The names of the qualified certificate profiles issued by the CAs appearing in this CPS are updated to better define their nature.</p> <p>All references to the STATUS platform are updated as Camerfirma STATUS®.</p> <p>1.3.1 The content of point 1.3.5.1 of the previous version is incorporated.</p> <p>1.3.5.7 its contents are moved to 1.3.1.1.</p> <p>1.5 Content is updated.</p> <p>The term 'hardware' is replaced by 'Card/Token' where deemed necessary.</p> <p>1.3.1.1.1.3.3.2.5 and 1.3.1.1.1.3.3.2.6 are updated in their wording.</p> <p>1.3.3.5.7.3.3.2.2 TSU certificates are eliminated.</p> <p>4.4.3 becomes not stipulated.</p> <p>5.2.1 The incompatibility between the role of CA Administrator and CA Operator is eliminated.</p> <p>5.4.3 The retention period of the audit logs is increased.</p> <p>5.7 Its content is updated.</p> <p>5.8 The content of the item is updated.</p> <p>6.6.2 The distribution of the contents of the item is updated.</p> <p>Minor changes in the wording of the document.</p> <p>The data on the creation, verification and approval of this CPS is updated on the cover page of the document.</p>
15/07/2022	V1.3.0	<p>This document changes its name from "CERTIFICATION PRACTICE STATEMENT DIGITAL CERTIFICATES AC CAMERFIRMA SA EIDAS" to "CERTIFICATION PRACTICE STATEMENT CAMERFIRMA 2003-2008-2016".</p>

		<p>This document is a continuation of the document "CERTIFICATION PRACTICE STATEMENT DIGITAL CERTIFICATES AC CAMERFIRMA SA EIDAS V1.2.20".</p> <p>Minor changes in the document's style and punctuation.</p> <p>1.1 Version update of the EN 319 401 reference version and additional content.</p> <p>1.3.1 Certification Authorities. Overall changes.</p> <p>3.2.3 Authentication of individual identity. More specificity in identification methods 2 and 3.</p> <p>3.2.5.1 Proof of relationship. Incorporation of code signing certificates.</p> <p>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'.</p> <p>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.</p> <p>4.9.3 Procedure for revocation request. Updating of procedures.</p> <p>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.</p> <p>4.9.7 CRL issuance frequency. Incorporation of the cases added to point '1.3.1 Certification Authorities' in this version of this document.</p> <p>6.1.1 Key pair generation. Incorporation of the cases added to point '1.3.1 Certification Authorities' in this version of this document.</p> <p>7.1.3 Algorithm object identifiers. Incorporation of the sha1WithRSAEncryption algorithm.</p>
23/08/2022	V1.3.1	<p>1.3.1.2 CHAMBERS OF COMMERCE ROOT HIERARCHIES, replacement of 'Certificado de TSU' with 'TSU Certificate'.</p> <p>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'</p> <p>1.3.1.2.2.1.8 Legal Person Certificate - Registered Professional Attribute, rewording of the text describing this profile.</p> <p>1.3.2 REGISTRATION AUTHORITY (RA), replacement of 'Delegate Agency' by 'Subsidiary'.</p> <p>1.6.1 ACRONYMS, 5.1.1 SITE LOCATION AND CONSTRUCTION, 5.1.2</p>

		<p>PHYSICAL ACCESS, the OCSP service is provided from AWS cloud.</p> <p>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.</p> <p>4.9.3 PROCEDURE FOR REVOCATION REQUEST, incorporation of revocation procedure through web service.</p> <p>5.4.3 RETENTION PERIOD FOR AUDIT LOGS, reduction of the retention period from 20 to 15 years.</p> <p>Minor changes in the wording of the document.</p> <p>Appendix I: document history, incorporation of the signing date of this document in its version 1.3.0</p>
31/03/2023	V1.4.0	<p>The document changes its name from "Certification Practice Statement CAMERFIRMA 2003-2008- 2016" to "Certification Practice Statement and Certificate Policies CAMERFIRMA 2008-2016".</p> <p>This version specifies the Camerfirma and Camerfirma Perú CPS and the Camerfirma CPs for Camerfirma and Camerfirma Perú active CAs under 2008 and 2016 Camerfirma hierarchies (Chambers of Commerce Root – 2008, CHAMBERS OF COMMERCE ROOT – 2016, Global Chambersign Root – 2008, GLOBAL CHAMBERSIGN ROOT – 2016).</p> <p>The document format is updated.</p> <p>Fixed the document code on the cover page (wrong in versions 1.3.0 and 1.3.1).</p> <p>The following terminated CAs, as specified in section 5.8.2 of this version, and their CPs are deleted:</p> <ul style="list-style-type: none"> - CHAMBERS OF COMMERCE ROOT – 2016 hierarchy: AC CAMERFIRMA FOR WEBSITES – 2016 (this CA is not included in versions 1.3.0 and 1.3.1 but it should be; although it had no active issued certificates, it was not yet terminated). - Chambers of Commerce Root hierarchy (2003 Camerfirma hierarchy, with no active CAs): AC Camerfirma Express Corporate Server, AC Camerfirma Certificados Camerales, Chambers of Commerce Root. - Global Chambersign Root – 2008 hierarchy: AC CAMERFIRMA – 2009, Entitat de Certificació de l'Administració Pública Andorrana-19, MULTICERT SSL Certification Authority 001, DigitalSign Primary CA, DigitalSign CA, DigitalSign TSA. - Global Chambersign Root hierarchy (2003 Camerfirma hierarchy, with no active CAs): RACER, AC Camerfirma, Global

		<p>Chambersign Root.</p> <p>The following terminated CPs (with no active certificates) are removed from active CAs:</p> <ul style="list-style-type: none"> - AC CAMERFIRMA AAPP II – 2014: 1.3.6.1.4.1.17326.1.3.3.1, 1.3.6.1.4.1.17326.1.3.4.1, 1.3.6.1.4.1.17326.1.3.4.2, 1.3.6.1.4.1.17326.1.3.4.3 <p>The following active CPs of active CAs are included, which are not included in versions 1.3.0 and 1.3.1 but they should be; although the CAs do not issue new certificates under these CPs, there are still active certificates issued by the CAs under these CPs that are about to expire:</p> <ul style="list-style-type: none"> - Camerfirma TSA II – 2014: 1.3.6.1.4.1.17326.10.13.1.2 (TSU Non-Qualified Certificate - P12). - Camerfirma TSA – 2013: 1.3.6.1.4.1.17326.10.13.1.3 (TSU Non-Qualified Certificate - HSM). <p>Revision and homogenization of terms and acronyms.</p> <p>References to internal Camerfirma documents are removed.</p> <p>1.1. Revision.</p> <p>1.2. Update. The name and description of the document is changed. The Camerfirma OIDs of the active CPs of the Camerfirma CAs under the 2008 and 2016 Camerfirma hierarchies are included.</p> <p>1.3 and all its sections. Revision and update.</p> <p>1.3.1.1, 1.3.1.2. All the CAs that operate under these hierarchies do so from infrastructures technically controlled by Camerfirma. Updating of CAs and CPs.</p> <p>1.3.1.1 and its sections, 1.3.1.2 and its sections. More identification details are added for the active Root CAs certificates of the hierarchies. The identification details for the Subordinate CAs certificates under this CPS within the hierarchies are added.</p> <p>1.3.1.3 OCSP certificates. New section.</p> <p>1.3.1.5. The CA CAMERFIRMA GESTIÓN INTERNA is out of scope of these CPS and CPs.</p> <p>1.3.2 RA. Nuevo PRV (Point of Remote Verification).</p> <p>1.3.3 Subscribers. Sections formerly in section 1.3.5 Other participants are incorporated. Changes in names of participants. The Subscriber participant is added.</p> <p>1.4.1, 1.4.2 Revision.</p>
--	--	---

	<p>1.6.1, 1.6.2. Revision and update. Change of order of sections.</p> <p>2 all sections. Revision and update. Changes in websites and web addresses. Changes in published information.</p> <p>3 and all sections. Review and update. Removal of sections 3.1.5.1, 3.2.5.3 and 3.2.5.4.</p> <p>3.2.3. The assisted process with pre-validation of documentation and synchronous mediation of an operator is removed as a remote identification process by video. The description of alternative methods for verifying the identity of the Applicant of a non-qualified certificate is added.</p> <p>4 and all its sections. Review and update.</p> <p>4.4.2. The CA will not make end entity certificates public, except for TSU certificates owned by Camerfirma.</p> <p>4.4.3. Notification to other entities of TSU, OCSP, Root CAs and Subordinate CAs certificates is added.</p> <p>4.5.1. Updating of CAs and CPs.</p> <p>4.6, 4.7. The content of section 4.6 is moved to section 4.7. The description of the process of re-keying a certificate in cases of certificate replacement is added.</p> <p>4.9.1. New circumstances for revocation.</p> <p>4.9.2. Changes to who can request revocation.</p> <p>4.9.3. Changes to procedures for revocation request. The procedure for revocation request made by the RA or the CA is described. New procedure for notification of events that may indicate the need for revocation of a certificate.</p> <p>4.9.4 Examples of specific cases that require a future revocation date are explained.</p> <p>4.9.5, 4.9.10. The maximum latency of the OCSP service for online CAs is changed to 10 minutes.</p> <p>4.9.7. Updating of CAs</p> <p>4.9.11. Revocation, suspension and reactivation notifications sent to the end entity certificate Subject and revocation notifications sent to the Subscriber of Subordinate CA and TSU certificates are described.</p> <p>4.9.15. The procedure for suspension request is corrected.</p> <p>4.10.2. The certificate status services are described in the event of termination of a CA under this CPS and in the event of cessation of Camerfirma's activity as a TSP.</p>
--	--

		<p>5.2.1. Alignment with the trusted roles in ETSI EN 319 401 and ETSI EN 319 411-1.</p> <p>5.2.3, 5.2.4. Revision.</p> <p>5.4.3, 5.5.1, 5.5.2. Revision.</p> <p>5.6. Revision and update. It includes notification of new CA certificates and termination of the CA.</p> <p>5.7.3. Review and update. It includes the termination of the CA with compromised key, the way in which the revocation status of certificates issued by the CA with compromised key continues to be provided, the revocation of an external Subordinate CA with compromised key and the replacement of the CA with compromised key.</p> <p>5.8. Review and update. The content of section 5.8 is divided into sections 5.8.1 Cessation of activity and 5.8.2 Termination of a CA. New section 5.8.3 Termination of a RA.</p> <p>6.1 and its sections. Review and update.</p> <p>6.1.1 Updating of CAs.</p> <p>6.2 and its sections. Revision and update.</p> <p>6.3.2. Revision and update. The period of validity of the certificates under these CPS and CPs is indicated.</p> <p>6.6. Revision.</p> <p>7 and its sections. Revision and update.</p> <p>7.2.2. CRL and CRL entry extensions are included.</p> <p>7.3.2. OCSP extensions are included.</p> <p>8 and its sections. Revision and update.</p> <p>8, 8.1, 8.2. Spanish National Security Scheme (ENS) audits are added.</p> <p>9.1.3, 9.3.3.1. Revision and update. Removal of websites.</p> <p>9.5. Revision.</p> <p>9.6 and its sections. Revision and update.</p> <p>9.7, 9.8. Revision.</p> <p>9.12.1, 9.12.2 and its sections, 9.12.3, 9.16.1. Revision.</p> <p>Other minor changes and corrections.</p>
26/02/2024	V1.5.0	<p>The document changes its name from "Certification Practice Statement and Certificate Policies CAMERFIRMA 2008-2016" to "Certification Practice Statement and Certificate Policies</p>

	<p>CAMERFIRMA" CAMERFIRMA".</p> <p>This document is a continuation of the document "Certification Practice Statement and Certificate Policies CAMERFIRMA 2008-2016 Version 1.4.0", incorporating the update content of the document "Certification Practice Statement and Certificate Policies CAMERFIRMA Version 1.1.0". These documents, as well as previous versions of these documents, can be consulted at:</p> <p>https://www.camerfirma.com/practicas-de-certificacion-ac-camerfirma-cps-dpc/practicas-de-certificacion-ac-camerfirma-cps-dpc-versiones-anteriores/.</p> <p>The content corresponding to Camerfirma Perú CPS is removed because its CAs are now governed by their own CPS.</p> <p>This version specifies the CPS and the CPs for the issuance of certificates by Camerfirma active CAs under 2008, 2016 and 2021 Camerfirma hierarchies (Chambers of Commerce Root – 2008, CHAMBERS OF COMMERCE ROOT – 2016, GLOBAL CHAMBERSIGN ROOT – 2016, CAMERFIRMA ROOT 2021, INFOCERT-CAMERFIRMA ROOT 2024).</p> <p>Updating of document location on the cover page.</p> <p>The following terminated CAs and, where applicable, their CPs are removed:</p> <ul style="list-style-type: none"> - CHAMBERS OF COMMERCE ROOT – 2016 hierarchy: IVSIGN CA. - Chambers of Commerce Root – 2008 hierarchy: Camerfirma TSA – 2013. - Global Chambersign Root – 2008 hierarchy: InfoCert Organization Validation CA 3, InfoCert Organization Validation 2019 CA 3. - Global Chambersign Root – 2008 hierarchy: InfoCert Organization Validation CA 3, InfoCert Organization Validation 2019 CA 3, GLOBAL CORPORATE SERVER, AC Camerfirma Portugal – 2015, Global Chambersign Root – 2008. <p>The following terminated CPs (with no active certificates) are removed from active CAs:</p> <ul style="list-style-type: none"> - Camerfirma TSA II – 2014: 1.3.6.1.4.1.17326.10.13.1.2 <p>The following CP are changed in active CAs:</p> <ul style="list-style-type: none"> - AC CAMERFIRMA FOR LEGAL PERSONS – 2016: 1.3.6.1.4.1.17326.10.16.2.2.1.4.3.1. QSCD SmartCard/Token (with no active certificates) is removed.
--	---

	<p>The following CAs are added:</p> <ul style="list-style-type: none"> - INFOCERT-CAMERFIRMA CERTIFICATES 2024. - INFOCERT-CAMERFIRMA TIMESTAMP 2024 <p>1.1. Revision. Removal of content corresponding to Camerfirma Perú CPS. Updating of hierarchies and ETSI standards versions. The types of QSCD and Non-QSCD devices on which the keys of the certificates issued by CAs under the CPS in this document are generated are added (they are removed in section 1.3.1.1).</p> <p>1.2. Removal of Camerfirma Perú CPS. Updating of hierarchies, CPs and document location. CPs Non-Qualified OCSP Certificate are added.</p> <p>1.3.1. Updating of Camerfirma's headquarter, telephone and email. Removal of content corresponding to Camerfirma Perú CPS. Incorporation of the CAMERFIRMA ROOT 2021 hierarchy.</p> <p>1.3.1.1. Removal of the types of QSCD and Non-QSCD devices on which the keys of the certificates issued by CAs under the CPS in this document are generated (they are added in section 1.1). Updating of CAs and CPs. CPs Non-Qualified OCSP Certificate are added.</p> <p>1.3.1.1.3 and its sections. Updating of CAs, CPs and FIPS.</p> <p>1.3.1.1.6 and its sections. Removal due to updating of CAs and CPs.</p> <p>1.3.1.2. Updating of CAs. Removal of content corresponding to Camerfirma Perú CPS and CPs. CPs Non-Qualified OCSP Certificate are added.</p> <p>1.3.1.2.2.1 and its sections. Removal due to to being content corresponding to Camerfirma Perú CPS and/or CPs.</p> <p>1.3.1.2.3, 1.3.1.2.4. Removal due to updating of CAs.</p> <p>New section 1.3.1.3, with its sections. Incorporation of the CAMERFIRMA ROOT 2021 hierarchy.</p> <p>1.3.1.5. Revision. Update due to incorporation of the CAMERFIRMA ROOT 2021 hierarchy. Generation and storage of OCSP certificates keys in an HSM FIPS 140-2 level 3 or CC EAL 4 or higher are added.</p> <p>1.3.2. Removal of content corresponding to Camerfirma Perú CPS.</p> <p>1.3.3.1, 1.3.3.2. Revision. Removal of content corresponding to Camerfirma Perú CPS.</p> <p>1.3.3.3, 1.3.3.4. Removal of content corresponding to Camerfirma Perú CPS.</p> <p>1.3.3.5. The <i>organizationIdenfier</i> attribute of the <i>subject</i> field is</p>
--	---

	<p>added as data of the Entity identified in a certificate.</p> <p>1.3.5.1. Removal of content corresponding to Camerfirma Perú CPS.</p> <p>1.4.2. Removal of content corresponding to Camerfirma Perú CPS.</p> <p>1.5.2. Updating of address, telephone and email.</p> <p>1.5.4. Updating of document location.</p> <p>1.6.1. Removal of content corresponding to Camerfirma Perú CPS. Definitions of end entity, end entity certificate and CA certificate are added.</p> <p>1.6.2. Removal of content corresponding to Camerfirma Perú CPS.</p> <p>2.2.1. Removal of content corresponding to Camerfirma Perú CPS.</p> <p>2.2.4, 2.3. Update due to Incorporation of the CAMERFIRMA ROOT 2021 hierarchy.</p> <p>3.1.1. Reviewed.</p> <p>3.2.2.1. Removal of content corresponding to Camerfirma Perú CPS.</p> <p>3.2.3. Revision. Removal of content corresponding to Camerfirma Perú CPS.</p> <p>3.3. Removal of content corresponding to Camerfirma Perú CPS.</p> <p>3.3.1. Revision.</p> <p>3.4. Removal of content corresponding to Camerfirma Perú CPS.</p> <p>4.1.2.3. Updating of FIPS.</p> <p>4.5.1. Updating of CAs and CPs. CPs Non-Qualified OCSP Certificate are added.</p> <p>4.7.1. Revision. Removal of content corresponding to Camerfirma Perú CPS.</p> <p>4.7.2. Removal of content corresponding to Camerfirma Perú CPS.</p> <p>4.7.3. Revision.</p> <p>4.9.1. Revision and update. Revocation causes aligned with <i>Mozilla Root Store Policy</i> are removed.</p> <p>4.9.2. Removal of content corresponding to Camerfirma Perú CPS.</p> <p>4.9.3. Revision. Removal of content corresponding to Camerfirma Perú CPS.</p> <p>4.9.4. Revision.</p> <p>4.9.5. Revision. Update due to Incorporation of the CAMERFIRMA ROOT 2021 hierarchy.</p>
--	---

	<p>4.9.7, 4.9.8, 4.9.10. Revision. Updating of CAs.</p> <p>4.9.13. Update due to Incorporation of the CAMERFIRMA ROOT 2021 hierarchy.</p> <p>4.9.14. Removal of content corresponding to Camerfirma Perú CPS.</p> <p>4.10.1, 4.10.2. Update due to Incorporation of the CAMERFIRMA ROOT 2021 hierarchy.</p> <p>5.5.1. Revision.</p> <p>5.7.3, 5.8.2. Update due to Incorporation of the CAMERFIRMA ROOT 2021 hierarchy.</p> <p>6.1.1. Updating of CAs.</p> <p>6.1.5. Revision.</p> <p>6.1.6. Revision. Update due to Incorporation of the CAMERFIRMA ROOT 2021 hierarchy.</p> <p>6.2.1.2. Updating of FIPS.</p> <p>6.3.2. Removal of content corresponding to Camerfirma Perú CPS.</p> <p>7.1.3. Revision. Update due to Incorporation of the CAMERFIRMA ROOT 2021 hierarchy.</p> <p>7.2.2. Update due to Incorporation of the CAMERFIRMA ROOT 2021 hierarchy.</p> <p>8, 8.1, 8.2, 8.4. Removal of content corresponding to Camerfirma Perú CPS.</p> <p>9.1.1. Removal of content corresponding to Camerfirma Perú CPS.</p> <p>9.1.4. Updating of these CPS and CPs location.</p> <p>9.1.5. Removal of content corresponding to Camerfirma Perú CPS.</p> <p>9.3.3.1. Update due to Incorporation of the CAMERFIRMA ROOT 2021 hierarchy.</p> <p>9.6.1.1, 9.8, 9.12.2.2. Removal of content corresponding to Camerfirma Perú CPS.</p> <p>Other minor changes and corrections.</p>
--	---