



AN INFOCERT COMPANY

**CERTIFICATION
PRACTICE STATEMENT
AND
CERTIFICATE POLICIES
CAMERFIRMA 2021
Version 1.1.0**

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://policy2021.camerfirma.com>

Language: English

Code: PUB-2022-18-10

INDEX

| | |
|--|-----------|
| 1. INTRODUCTION | 12 |
| 1.1 OVERVIEW | 12 |
| 1.2 DOCUMENT NAME AND IDENTIFICATION | 14 |
| 1.3 PKI PARTICIPANTS | 15 |
| 1.3.1 CERTIFICATION AUTHORITIES (CAS) | 15 |
| 1.3.1.1 CAMERFIRMA ROOT 2021 Hierarchy | 16 |
| 1.3.1.2 OCSP certificates | 22 |
| 1.3.1.3 Test certificates | 23 |
| 1.3.2 REGISTRATION AUTHORITIES (RAS) | 23 |
| 1.3.3 SUBSCRIBERS | 25 |
| 1.3.3.1 Subscriber | 25 |
| 1.3.3.2 Subject, Signatory and Creator of a Seal | 26 |
| 1.3.3.3 Applicant | 27 |
| 1.3.3.4 Person Responsible | 27 |
| 1.3.3.5 Entity | 28 |
| 1.3.4 RELYING PARTIES | 28 |
| 1.3.5 OTHER PARTICIPANTS | 28 |
| 1.3.5.1 Supervisory Body | 28 |
| 1.3.5.2 Trust Service Provider (TSP) and Qualified Trust Service Provider (QTSP) | 29 |
| 1.4 CERTIFICATE USAGE | 29 |
| 1.4.1 APPROPRIATE CERTIFICATE USES | 30 |
| 1.4.2 PROHIBITED CERTIFICATE USES | 30 |
| 1.5 POLICY ADMINISTRATION | 31 |
| 1.5.1 ORGANIZATION ADMINISTERING THE DOCUMENT | 31 |
| 1.5.2 CONTACT PERSON | 31 |
| 1.5.3 PERSON DETERMINING CPS SUITABILITY FOR THE POLICY | 31 |
| 1.5.4 CPS APPROVAL PROCEDURES | 31 |
| 1.6 DEFINITIONS AND ACRONYMS | 31 |
| 1.6.1 DEFINITIONS | 32 |
| 1.6.2 ACRONYMS | 36 |
| 2. PUBLICATION AND REPOSITORY RESPONSIBILITIES | 39 |
| 2.1 REPOSITORIES | 39 |
| 2.2 PUBLICATION OF CERTIFICATION INFORMATION | 39 |
| 2.2.1 CERTIFICATION PRACTICES AND CERTIFICATE POLICIES | 39 |

| | | |
|---------|--|----|
| 2.2.2 | TERMS AND CONDITIONS | 39 |
| 2.2.3 | DISTRIBUTION OF THE CERTIFICATES | 39 |
| 2.2.4 | CRL AND OCSP | 40 |
| 2.3 | TIME OR FREQUENCY OF PUBLICATION | 41 |
| 2.4 | ACCESS CONTROLS ON REPOSITORIES | 41 |
| 3. | IDENTIFICATION AND AUTHENTICATION | 42 |
| 3.1 | NAMING | 42 |
| 3.1.1 | TYPES OF NAMES | 42 |
| 3.1.2 | NEED FOR NAMES TO BE MEANINGFUL | 42 |
| 3.1.3 | ANONYMITY OR PSEUDONYMITY OF SUBSCRIBERS | 42 |
| 3.1.4 | RULES FOR INTERPRETING VARIOUS NAME FORMS | 43 |
| 3.1.5 | UNIQUENESS OF NAMES | 43 |
| 3.1.6 | RECOGNITION, AUTHENTICATION, AND ROLE OF TRADEMARKS | 43 |
| 3.1.7 | NAME DISPUTE RESOLUTION PROCEDURE | 43 |
| 3.2 | INITIAL IDENTITY VALIDATION | 43 |
| 3.2.1 | METHOD TO PROVE POSSESSION OF THE PRIVATE KEY | 43 |
| 3.2.2 | AUTHENTICATION OF ORGANIZATION IDENTITY | 44 |
| 3.2.2.1 | Identity | 44 |
| 3.2.2.2 | Trademarks | 44 |
| 3.2.2.3 | Country verification | 44 |
| 3.2.2.4 | Validation of domain authorization or control | 44 |
| 3.2.2.5 | Authentication of an IP address | 45 |
| 3.2.2.6 | Wildcard Domain Validation | 45 |
| 3.2.2.7 | Accuracy of data sources | 45 |
| 3.2.2.8 | CAA | 45 |
| 3.2.3 | AUTHENTICATION OF INDIVIDUAL IDENTITY | 45 |
| 3.2.4 | NON-VERIFIED SUBSCRIBER INFORMATION | 47 |
| 3.2.5 | VALIDATION OF AUTHORITY | 47 |
| 3.2.5.1 | Verification of association of the Applicant with the Entity | 47 |
| 3.2.5.2 | Service or Machine Identity | 48 |
| 3.2.5.3 | Special considerations for issuing certificates outside of Spanish territory | 48 |
| 3.2.6 | CRITERIA FOR INTEROPERATION | 48 |
| 3.3 | IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS | 49 |
| 3.3.1 | IDENTIFICATION AND AUTHENTICATION FOR ROUTINE RE-KEY | 49 |
| 3.3.2 | IDENTIFICATION AND AUTHENTICATION FOR RE-KEY AFTER REVOCATION | 49 |

| | | |
|---------|---|----|
| 3.4 | IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST | 49 |
| 4. | CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS | 50 |
| 4.1 | CERTIFICATE APPLICATION | 50 |
| 4.1.1 | WHO CAN SUBMIT A CERTIFICATE APPLICATION | 50 |
| 4.1.2 | ENROLLMENT PROCESS AND RESPONSIBILITIES | 50 |
| 4.2 | CERTIFICATE APPLICATION PROCESSING | 50 |
| 4.2.1 | PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS | 51 |
| 4.2.2 | APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS | 51 |
| 4.2.3 | TIME TO PROCESS CERTIFICATE APPLICATIONS | 51 |
| 4.2.4 | NOTIFICATION TO THE SUBSCRIBER BY THE CA OF ISSUANCE OF A CERTIFICATE | 52 |
| 4.3 | CERTIFICATE ISSUANCE | 52 |
| 4.3.1 | CA ACTIONS DURING CERTIFICATE ISSUANCE | 52 |
| 4.3.1.1 | Certificates issued on QSCD SmartCard/Token | 52 |
| 4.3.1.2 | Certificates on QSCD Cloud (HSM) | 52 |
| 4.3.1.3 | Certificates issued for testing purposes | 52 |
| 4.3.2 | NOTIFICATION TO SUBSCRIBER BY THE CA OF ISSUANCE OF CERTIFICATE | 53 |
| 4.3.3 | ACTIVATION | 53 |
| 4.3.3.1 | Activation of the signature device (smartcard or token) | 53 |
| 4.3.3.2 | Activation of the remote signature device (HSM) | 53 |
| 4.4 | CERTIFICATE ACCEPTANCE | 53 |
| 4.4.1 | CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE | 53 |
| 4.4.2 | PUBLICATION OF THE CERTIFICATE BY THE CA | 54 |
| 4.4.3 | NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES | 54 |
| 4.5 | KEY PAIR AND CERTIFICATE USAGE | 54 |
| 4.5.1 | SUBSCRIBER PRIVATE KEY AND CERTIFICATE USAGE | 54 |
| 4.5.2 | THE RELYING PARTY PUBLIC KEY AND CERTIFICATE USAGE | 55 |
| 4.6 | CERTIFICATE RENEWAL | 56 |
| 4.6.1 | CIRCUMSTANCE FOR CERTIFICATE RENEWAL | 56 |
| 4.6.2 | WHO MAY REQUEST RENEWAL | 56 |
| 4.6.3 | PROCESSING CERTIFICATE RENEWAL REQUESTS | 56 |
| 4.6.4 | NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER | 56 |
| 4.6.5 | CONDUCT CONSTITUTING ACCEPTANCE OF A RENEWAL CERTIFICATE | 56 |
| 4.6.6 | PUBLICATION OF THE RENEWAL CERTIFICATE BY THE CA | 56 |
| 4.6.7 | NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES | 56 |
| 4.7 | CERTIFICATE RE-KEY | 57 |

| | | |
|--------|--|----|
| 4.7.1 | CIRCUMSTANCE FOR CERTIFICATE RE-KEY | 57 |
| 4.7.2 | WHO MAY REQUEST CERTIFICATION OF A NEW PUBLIC KEY | 57 |
| 4.7.3 | PROCESSING CERTIFICATE RE-KEY REQUESTS | 57 |
| 4.7.4 | NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER..... | 57 |
| 4.7.5 | CONDUCT CONSTITUTING ACCEPTANCE OF A RE-KEYED CERTIFICATE | 58 |
| 4.7.6 | PUBLICATION OF THE RE-KEYED CERTIFICATE BY THE CA..... | 58 |
| 4.7.7 | NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES | 58 |
| 4.8 | CERTIFICATE MODIFICATION | 58 |
| 4.8.1 | CIRCUMSTANCE FOR CERTIFICATE MODIFICATION | 58 |
| 4.8.2 | WHO MAY REQUEST CERTIFICATE MODIFICATION | 58 |
| 4.8.3 | PROCESSING CERTIFICATE MODIFICATION REQUESTS | 58 |
| 4.8.4 | NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER..... | 58 |
| 4.8.5 | CONDUCT CONSTITUTING ACCEPTANCE OF MODIFIED CERTIFICATE | 59 |
| 4.8.6 | PUBLICATION OF THE MODIFIED CERTIFICATE BY THE CA..... | 59 |
| 4.8.7 | NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES | 59 |
| 4.9 | CERTIFICATE REVOCATION AND SUSPENSION..... | 59 |
| 4.9.1 | CIRCUMSTANCES FOR REVOCATION | 59 |
| 4.9.2 | WHO CAN REQUEST REVOCATION | 62 |
| 4.9.3 | PROCEDURE FOR REVOCATION REQUEST | 62 |
| 4.9.4 | REVOCATION REQUEST GRACE PERIOD | 66 |
| 4.9.5 | TIME WITHIN WHICH CA MUST PROCESS THE REVOCATION REQUEST | 66 |
| 4.9.6 | REVOCATION CHECKING REQUIREMENT FOR THE RELYING PARTIES | 67 |
| 4.9.7 | CRL ISSUANCE FREQUENCY | 67 |
| 4.9.8 | MAXIMUM LATENCY FOR CRLS..... | 67 |
| 4.9.9 | ONLINE REVOCATION/STATUS CHECKING AVAILABILITY | 68 |
| 4.9.10 | ONLINE REVOCATION CHECKING REQUIREMENTS | 68 |
| 4.9.11 | OTHER FORMS OF REVOCATION ADVERTISEMENTS AVAILABLE | 68 |
| 4.9.12 | SPECIAL REQUIREMENTS REGARDING PRIVATE KEY COMPROMISE | 69 |
| 4.9.13 | CIRCUMSTANCES FOR SUSPENSION..... | 69 |
| 4.9.14 | WHO CAN REQUEST SUSPENSION..... | 69 |
| 4.9.15 | PROCEDURE FOR SUSPENSION REQUEST..... | 69 |
| 4.9.16 | LIMITS ON SUSPENSION PERIOD..... | 69 |
| 4.10 | CERTIFICATE STATUS SERVICES | 69 |
| 4.10.1 | OPERATIONAL CHARACTERISTICS | 69 |
| 4.10.2 | SERVICE AVAILABILITY | 70 |
| 4.10.3 | OPTIONAL FEATURES..... | 70 |

| | | |
|--------|---|----|
| 4.11 | END OF SUBSCRIPTION | 70 |
| 4.12 | KEY ESCROW AND RECOVERY | 71 |
| 4.12.1 | KEY ESCROW AND RECOVERY POLICY AND PRACTICES | 71 |
| 4.12.2 | SESSION KEY ENCAPSULATION AND RECOVERY POLICY AND PRACTICES | 71 |
| 5. | FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS | 72 |
| 5.1 | PHYSICAL CONTROLS | 72 |
| 5.1.1 | SITE LOCATION AND CONSTRUCTION | 72 |
| 5.1.2 | PHYSICAL ACCESS | 73 |
| 5.1.3 | POWER AND AIR CONDITIONING..... | 73 |
| 5.1.4 | WATER EXPOSURES | 74 |
| 5.1.5 | FIRE PREVENTION AND PROTECTION | 74 |
| 5.1.6 | MEDIA STORAGE | 74 |
| 5.1.7 | WASTE DISPOSAL..... | 75 |
| 5.1.8 | OFF-SITE BACKUP..... | 75 |
| 5.2 | PROCEDURAL CONTROLS..... | 75 |
| 5.2.1 | TRUSTED ROLES | 75 |
| 5.2.2 | NUMBER OF PERSONS REQUIRED PER TASK | 76 |
| 5.2.3 | IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE | 76 |
| 5.2.4 | ROLES REQUIRING SEPARATION OF DUTIES..... | 76 |
| 5.3 | PERSONNEL CONTROLS | 76 |
| 5.3.1 | QUALIFICATIONS, EXPERIENCE, AND CLEARANCE REQUIREMENTS | 76 |
| 5.3.2 | BACKGROUND CHECK PROCEDURES | 77 |
| 5.3.3 | TRAINING REQUIREMENTS | 77 |
| 5.3.4 | RETRAINING FREQUENCY AND REQUIREMENTS | 78 |
| 5.3.5 | JOB ROTATION FREQUENCY AND SEQUENCE | 78 |
| 5.3.6 | SANCTIONS FOR UNAUTHORIZED ACTIONS | 79 |
| 5.3.7 | INDEPENDENT CONTRACTOR REQUIREMENTS | 79 |
| 5.3.8 | DOCUMENTATION SUPPLIED TO PERSONNEL | 79 |
| 5.4 | AUDIT LOGGING PROCEDURES | 80 |
| 5.4.1 | TYPES OF EVENTS RECORDED | 80 |
| 5.4.2 | FREQUENCY OF PROCESSING LOG | 80 |
| 5.4.3 | RETENTION PERIOD FOR AUDIT LOGS..... | 80 |
| 5.4.4 | PROTECTION OF AUDIT LOG | 80 |
| 5.4.5 | AUDIT LOG BACKUP PROCEDURES..... | 80 |
| 5.4.6 | AUDIT COLLECTION SYSTEM (INTERNAL VS. EXTERNAL) | 81 |

| | | |
|---------|---|----|
| 5.4.7 | NOTIFICATION TO EVENT-CAUSING SUBJECT | 81 |
| 5.4.8 | VULNERABILITY ASSESSMENTS | 81 |
| 5.5 | RECORDS ARCHIVAL | 81 |
| 5.5.1 | TYPES OF RECORDS ARCHIVED..... | 81 |
| 5.5.2 | RETENTION PERIOD FOR ARCHIVE | 81 |
| 5.5.3 | PROTECTION OF ARCHIVE | 81 |
| 5.5.4 | ARCHIVE BACKUP PROCEDURES | 82 |
| 5.5.5 | REQUIREMENTS FOR TIME-STAMPING OF RECORDS | 82 |
| 5.5.6 | ARCHIVE COLLECTION SYSTEM (INTERNAL OR EXTERNAL) | 82 |
| 5.5.7 | PROCEDURES TO OBTAIN AND VERIFY ARCHIVE INFORMATION | 82 |
| 5.6 | KEY CHANGEOVER..... | 82 |
| 5.7 | COMPROMISE AND DISASTER RECOVERY | 83 |
| 5.7.1 | INCIDENT AND COMPROMISE HANDLING PROCEDURES | 83 |
| 5.7.2 | COMPUTING RESOURCES, SOFTWARE, AND/OR DATA ARE CORRUPTED | 83 |
| 5.7.3 | ENTITY PRIVATE KEY COMPROMISE PROCEDURES..... | 83 |
| 5.7.4 | BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER..... | 85 |
| 5.8 | CA OR RA TERMINATION | 85 |
| 5.8.1 | CESSATION OF ACTIVITY | 85 |
| 5.8.2 | TERMINATION OF A CA..... | 86 |
| 5.8.3 | TERMINATION OF A RA..... | 88 |
| 6. | TECHNICAL SECURITY CONTROLS | 89 |
| 6.1 | KEY PAIR GENERATION AND INSTALLATION | 89 |
| 6.1.1 | KEY PAIR GENERATION | 89 |
| 6.1.1.1 | Creating the Subject's key pair | 89 |
| 6.1.1.2 | Key creation hardware/software..... | 90 |
| 6.1.2 | PRIVATE KEY DELIVERY TO THE SUBSCRIBER | 90 |
| 6.1.3 | PUBLIC KEY DELIVERY TO THE CERTIFICATE ISSUER..... | 90 |
| 6.1.4 | CA PUBLIC KEY DELIVERY TO THE RELYING PARTIES..... | 90 |
| 6.1.5 | KEY SIZES | 90 |
| 6.1.6 | PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING | 91 |
| 6.1.7 | KEY USAGE PURPOSES (AS PER X.509 V3 KEY USAGE FIELD) | 91 |
| 6.2 | PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS..... | 91 |
| 6.2.1 | CRYPTOGRAPHIC MODULE STANDARDS AND CONTROLS | 91 |
| 6.2.2 | PRIVATE KEY (N OUT OF M) MULTI-PERSON CONTROL | 92 |
| 6.2.3 | PRIVATE KEY ESCROW | 92 |

| | | |
|---------|--|----|
| 6.2.4 | PRIVATE KEY BACKUP | 92 |
| 6.2.5 | PRIVATE KEY ARCHIVAL | 92 |
| 6.2.6 | PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE | 92 |
| 6.2.7 | PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE | 92 |
| 6.2.8 | METHOD OF ACTIVATING PRIVATE KEY | 92 |
| 6.2.9 | METHOD OF DEACTIVATING PRIVATE KEY | 93 |
| 6.2.10 | METHOD OF DESTROYING PRIVATE KEY | 93 |
| 6.2.11 | CRYPTOGRAPHIC MODULE RATING | 93 |
| 6.3 | OTHER ASPECTS OF KEY PAIR MANAGEMENT..... | 93 |
| 6.3.1 | PUBLIC KEY ARCHIVAL | 93 |
| 6.3.2 | CERTIFICATE OPERATIONAL PERIODS AND KEY PAIR USAGE PERIODS | 93 |
| 6.4 | ACTIVATION DATA | 94 |
| 6.5 | COMPUTER SECURITY CONTROLS | 94 |
| 6.5.1 | SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS | 94 |
| 6.5.2 | COMPUTER SECURITY RATING | 94 |
| 6.6 | LIFE CYCLE TECHNICAL CONTROLS..... | 94 |
| 6.6.1 | SYSTEM DEVELOPMENT CONTROLS..... | 95 |
| 6.6.2 | SECURITY MANAGEMENT CONTROLS | 95 |
| 6.6.2.1 | Security management | 95 |
| 6.6.2.2 | Data and asset classification and management | 95 |
| 6.6.2.3 | Management procedures | 95 |
| 6.6.2.4 | Access system management..... | 96 |
| 6.6.2.5 | Managing the cryptographic hardware lifecycle | 96 |
| 6.6.3 | LIFE CYCLE SECURITY CONTROLS..... | 97 |
| 6.7 | NETWORK SECURITY CONTROLS | 97 |
| 6.8 | TIME-STAMPING | 97 |
| 7. | CERTIFICATE, CRL, AND OCSP PROFILES..... | 98 |
| 7.1 | CERTIFICATE PROFILE | 98 |
| 7.1.1 | VERSION NUMBER..... | 98 |
| 7.1.2 | CERTIFICATE EXTENSIONS..... | 98 |
| 7.1.3 | ALGORITHM OBJECT IDENTIFIERS | 98 |
| 7.1.4 | NAME FORMS..... | 98 |
| 7.1.5 | NAME CONSTRAINTS | 99 |
| 7.1.6 | CERTIFICATE POLICY OBJECT IDENTIFIER..... | 99 |
| 7.1.7 | USAGE OF POLICY CONSTRAINTS EXTENSION | 99 |

| | | |
|-------|--|-----|
| 7.1.8 | POLICY QUALIFIERS SYNTAX AND SEMANTICS | 99 |
| 7.1.9 | PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICIES EXTENSION | 100 |
| 7.2 | CRL PROFILE | 100 |
| 7.2.1 | VERSION NUMBER | 100 |
| 7.2.2 | CRL AND CRL ENTRY EXTENSIONS | 100 |
| 7.3 | OCSP PROFILE | 100 |
| 7.3.1 | VERSION NUMBER | 101 |
| 7.3.2 | OCSP EXTENSIONS | 101 |
| 8. | COMPLIANCE AUDIT AND OTHER ASSESSMENTS | 102 |
| 8.1 | FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT | 102 |
| 8.1.1 | EXTERNAL SUBORDINATE CA AUDITS OR CROSS-CERTIFICATION | 103 |
| 8.1.2 | AUDITING THE RAS | 103 |
| 8.1.3 | SELF-AUDITS | 103 |
| 8.2 | IDENTITY/QUALIFICATIONS OF ASSESSOR | 103 |
| 8.3 | ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY | 103 |
| 8.4 | TOPICS COVERED BY THE ASSESSMENT | 104 |
| 8.5 | ACTIONS TAKEN AS A RESULT OF DEFICIENCY | 104 |
| 8.6 | COMMUNICATION OF RESULTS | 104 |
| 9. | OTHER BUSINESS AND LEGAL MATTERS | 106 |
| 9.1 | FEES | 106 |
| 9.1.1 | CERTIFICATE ISSUANCE OR RENEWAL FEES | 106 |
| 9.1.2 | CERTIFICATE ACCESS FEES | 106 |
| 9.1.3 | REVOCATION OR STATUS INFORMATION ACCESS FEES | 106 |
| 9.1.4 | FEES FOR OTHER SERVICES | 106 |
| 9.1.5 | REFUND POLICY | 106 |
| 9.2 | FINANCIAL RESPONSIBILITY | 106 |
| 9.2.1 | INSURANCE COVERAGE | 106 |
| 9.2.2 | OTHER ASSETS | 107 |
| 9.2.3 | INSURANCE OR WARRANTY COVERAGE FOR END-ENTITIES | 107 |
| 9.3 | CONFIDENTIALITY OF BUSINESS INFORMATION | 107 |
| 9.3.1 | SCOPE OF BUSINESS INFORMATION | 107 |
| 9.3.2 | INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION | 107 |
| 9.3.3 | RESPONSIBILITY TO PROTECT CONFIDENTIAL INFORMATION | 108 |
| 9.4 | PRIVACY OF PERSONAL INFORMATION | 108 |
| 9.4.1 | PRIVACY PLAN | 108 |

| | | |
|----------|---|-----|
| 9.4.2 | INFORMATION TREATED AS PRIVATE | 108 |
| 9.4.3 | INFORMATION NOT DEEMED PRIVATE | 108 |
| 9.4.4 | RESPONSIBILITY TO PROTECT PRIVATE INFORMATION | 108 |
| 9.4.5 | NOTICE AND CONSENT TO USE PRIVATE INFORMATION | 108 |
| 9.4.6 | DISCLOSURE PURSUANT TO JUDICIAL OR ADMINISTRATIVE PROCESS | 109 |
| 9.4.7 | OTHER INFORMATION DISCLOSURE CIRCUMSTANCES..... | 109 |
| 9.5 | INTELLECTUAL PROPERTY RIGHTS | 109 |
| 9.6 | REPRESENTATIONS AND WARRANTIES..... | 109 |
| 9.6.1 | CA REPRESENTATIONS AND WARRANTIES..... | 109 |
| 9.6.1.1 | CAs under this CPS..... | 109 |
| 9.6.1.2 | External Subordinate CAs | 111 |
| 9.6.2 | RA REPRESENTATIONS AND WARRANTIES..... | 112 |
| 9.6.3 | SUBSCRIBER REPRESENTATIONS AND WARRANTIES..... | 113 |
| 9.6.3.1 | Subscriber | 113 |
| 9.6.3.2 | Applicant | 114 |
| 9.6.3.3 | Subject and Person Responsible | 114 |
| 9.6.3.4 | Entity..... | 115 |
| 9.6.4 | RELYING PARTY REPRESENTATIONS AND WARRANTIES | 116 |
| 9.6.5 | REPRESENTATIONS AND WARRANTIES OF OTHER PARTICIPANTS | 116 |
| 9.7 | DISCLAIMERS OF WARRANTIES..... | 116 |
| 9.8 | LIMITATIONS OF LIABILITY | 117 |
| 9.8.1 | CA LIMITATIONS OF LIABILITY | 118 |
| 9.8.2 | RA LIMITATIONS OF LIABILITY | 118 |
| 9.8.3 | SUBSCRIBER, APPLICANT, SUBJECT, PERSON RESPONSIBLE AND ENTITY LIMITATIONS OF LIABILITY 118 | |
| 9.8.4 | CAMERFIRMA LIMITATIONS OF LIABILITY | 118 |
| 9.9 | INDEMNITIES | 119 |
| 9.10 | TERM AND TERMINATION | 119 |
| 9.10.1 | TERM..... | 120 |
| 9.10.2 | TERMINATION | 120 |
| 9.10.3 | EFFECT OF TERMINATION AND SURVIVAL | 120 |
| 9.11 | INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS..... | 120 |
| 9.12 | AMENDMENTS..... | 120 |
| 9.12.1 | PROCEDURE FOR AMENDMENT..... | 120 |
| 9.12.2 | NOTIFICATION MECHANISM AND PERIOD | 120 |
| 9.12.2.1 | List of aspects..... | 120 |

| | | |
|------------------------------------|--|-----|
| 9.12.2.2 | Notification method | 121 |
| 9.12.2.3 | Period for comments | 121 |
| 9.12.2.4 | Comment processing system | 121 |
| 9.12.3 | CIRCUMSTANCES UNDER WHICH OID MUST BE CHANGED | 121 |
| 9.13 | DISPUTE RESOLUTION PROCEDURE | 121 |
| 9.14 | GOVERNING LAW | 121 |
| 9.15 | COMPLIANCE WITH APPLICABLE LAW | 121 |
| 9.16 | MISCELLANEOUS PROVISIONS | 122 |
| 9.16.1 | ENTIRE AGREEMENT | 122 |
| 9.16.2 | ASSIGNMENT | 122 |
| 9.16.3 | SEVERABILITY | 122 |
| 9.16.4 | ENFORCEMENT (ATTORNEYS' FEES AND WAIVER OF RIGHTS) | 122 |
| 9.17 | OTHER PROVISIONS | 122 |
| APPENDIX I: DOCUMENT HISTORY | | 123 |

1. INTRODUCTION

1.1 OVERVIEW

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

Certificate Policy (hereinafter, CP): a set of rules defining the applicability of a 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 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 AC Camerfirma SA (hereinafter, Camerfirma) CPS and CPs for the issuance of certificates by Camerfirma active CAs under 2021 Camerfirma hierarchy (CAMERFIRMA ROOT 2021), in accordance with eIDAS Regulation and based on the following ETSI standards:

| Service | ETSI general | ETSI scope | ETSI profiles |
|---|--|--|--|
| Issuance of 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; Part 1: General Providers issuing certificates 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 v1.4.4: Certificate Profiles; Part 1: Overview and common data structures EN 319 412-2 v2.2.1: Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons EN 319 412-5 v2.3.1: Certificate Profiles; Part 5: QcStatements |
| Issuance of CA certificates to legal persons (certificates for electronic seals, 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 | |

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 27 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. |

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

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

1.2 DOCUMENT NAME AND IDENTIFICATION

| | |
|--------------|--|
| Name: | Certification Practice Statement and Certificate Policies CAMERFIRMA 2021 |
| Description: | Certification Practice Statement and Certificate Policies for Camerfirma active CAs under 2021 Camerfirma hierarchy (CAMERFIRMA ROOT 2021) |
| Version: | See homepage |
| OIDs: | <ul style="list-style-type: none"> • 1.3.6.1.4.1.17326.10.21.1: CPS • CPs Qualified Citizen Certificate <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 • CPs Qualified Corporate Certificate <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 <ul style="list-style-type: none"> ○ Legal Representative of a Legal Entity <ul style="list-style-type: none"> ▪ 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 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

Location: <https://policy2021.camerfirma.com>

1.3 PKI PARTICIPANTS

1.3.1 CERTIFICATION AUTHORITIES (CAS)

A CA is a component of a PKI responsible for issuing and managing 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 certificate.

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

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

Corporate name: AC CAMERFIRMA, S.A.

Tax number (NIF): A82743287

Headquarter: Calle Ribera del Loira 12 - 28042 Madrid

Telephone: +34 91 344 37 43

Email: ca@camerfirma.com

Webpage: <https://www.camerfirma.com>

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

A CA uses Registration Authorities (hereinafter, RA or RAs) for checking and storing end entity

certificates content documentation. 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 or other Subordinate CA certificates. The number of Subordinate CAs allowed under a Root or Subordinate CA has been specified in the *Basic Constraints (pathLenConstraint)* extension of the CA certificate.

The following section 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 hierarchy:

- CAMERFIRMA ROOT 2021

1.3.1.1 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 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 - | Qualified Certificate for a Legal Representative of a Non-Legal Entity - |

| | |
|---|---|
| representative of a non-legal entity] 0.4.0.194112.1.2 [ETSI EN 319 411-2 - QCP-n-qscd] | 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 - 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 |
| 1.3.6.1.4.1.17326.10.21.1.6.1 [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 |

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.

1.3.1.1.1 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 0FFF AC31 6B34

This CA issues different types of qualified certificates on QSCD devices, the keys of which are generated in:

- QSCD SmartCard/Token:
 - QSCD cryptographic smartcards.
 - QSCD cryptographic tokens.
- QSCD Cloud:
 - QSCD centralized platform managed by Camerfirma or another QTSP.

The CPs of the active certificates issued by this Subordinate CA are:

1.3.1.1.1.1 QUALIFIED CITIZEN CERTIFICATE

This qualified certificate identifies a natural person (Subject/Signatory) only to act on his/her own behalf.

1.3.1.1.1.2 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.

1.3.1.1.1.3 QUALIFIED CERTIFICATES FOR A REPRESENTATIVE

1.3.1.1.3.1 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 and 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.

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.

1.3.1.1.3.2 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.

1.3.1.1.1.3.3 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.

1.3.1.1.1.3.4 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.

1.3.1.1.3.5 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.

1.3.1.1.3.6 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.

1.3.1.2 OCSP CERTIFICATES

Every Root CA and every Subordinate CA under this CPS issues an 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 and on the status *unknown* of certificates issued by any other CA.

In the event of termination of a CA under this CPS for a reason other than the compromise of its private key (see section 5.8.2), the CA's OCSP service will no longer be available at its access address.

In the event of termination of a CA under this CPS for compromise of its private key (see section 5.7.3), the CA's OCSP service will continue to provide information on the status of certificates issued by the CA and on the status *unknown* of certificates issued by any other CA at the same access address, but the service's responses will be signed with a *default* OCSP certificate issued by another Camerfirma Subordinate CA. In the event of cessation of Camerfirma's activity as a TSP (see section 5.8.1), the CA's OCSP service will no longer be available at its access address.

The OID of all OCSP certificates issued by CAs under this CPS is 1.3.6.1.4.1.17326.10.21.0.1.

1.3.1.3 TEST CERTIFICATES

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

Name of the Entity: **[SOLO PRUEBAS] ENTIDAD**
Entity 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 before in the name of the Entity and in the CN to identify at first sight that it is a test certificate without liability.

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 Subordinate 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.

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 the 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 and registration 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, and checking its suitability for the type of certificate requested, but a PPV 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, and deliver the evidence of the identification to the RA. 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, and checking its suitability for the type of certificate requested, 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), to any Subscriber obligation for one or more certificates.

The Subscriber is, where applicable, the party that contracts Camerfirma 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.

- 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) with which the natural person is associated.
 - A legal person (other than, where applicable, the legal person Entity with which the natural person is associated).

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

- A third party organization acting as the RA 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.
- 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 with which the natural person is associated (the legal person or the non-legal entity identified in the certificate).
 - A legal person (other than, where applicable, the legal person identified in the certificate).

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:
 - The Signatory is the natural person Subject (the natural person identified in the certificate).
 - There is no Creator of a Seal.

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.

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.

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 defined in the *Organization* field (O) 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).

1.3.4 RELYING PARTIES

In these CPS and CP, the Relying 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 Trust 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 PSC (CA), and to other TSPs and QTSPs.

1.4 CERTIFICATE USAGE

1.4.1 APPROPRIATE CERTIFICATE USES

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

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

1.4.2 PROHIBITED CERTIFICATE USES

Camerfirma includes information on the limitation of use in the certificate, either in 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 are not authorized for use or resale as monitoring equipment for dangerous situations or for uses requiring fail-safe actions, such as the operation of nuclear facilities, navigation systems or aerial communication, or weapons control systems, where failure could lead directly to death, personal injury or severe environmental damage.

The use of 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 and with the Subscribers is considered illegal, and the CAs are exempt from any liability due to the Subject or third party's misuse of the certificates in accordance with current law.

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

The private key of the certificates is stored by Camerfirma only for the certificates in QSCD 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 Ribera del Loira, 12. Madrid (Spain)

Phone: +34 91 344 37 43

Email: compliance@camerfirma.com

Webpage: <https://www.camerfirma.com>

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

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

1.5.3 PERSON DETERMINING CPS SUITABILITY FOR THE POLICY

The legal department of Camerfirma is therefore constituted in the Policy Authority (PA) of the CA hierarchies described above being responsible for the suitability of the CPS and CPs in this document.

1.5.4 CPS APPROVAL PROCEDURES

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

AC Camerfirma publishes every new version of this document on its website <https://policy2021.camerfirma.com>. 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: 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 signature | Electronic signature which meets the requirements set out in Article 26 of 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. |
| 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 Practices | Set of practices adopted by a Certification Authority for the issuance, management, revocation, and renewal or re-key of certificates. |

| Statement | |
|--------------------------------------|---|
| 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: a) that the data has not been modified (integrity); b) that the person signing the data is who he/she claims (identification); and c) that the person signing the data cannot deny having done so (non-repudiation at origin). |
| 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. |
| Entity | Public or private, individual or collective organization, recognized in law, as defined in the <i>Organization</i> field (O) 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 an 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 signatures, 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 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 | Entity responsible for managing requests, identification and registration of |

| | |
|-----------------------------|---|
| Authority | 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: 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. |
| 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 |

| | |
|-----------------|--|
| Validation data | Data that is used to validate an electronic signature or an electronic seal. Also called public key. |
|-----------------|--|

1.6.2 ACRONYMS

| | |
|---------|---|
| AgID | <i>Agenzia per l'Italia Digitale</i> (national Supervisory Body in Italy) |
| 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. List of revoked certificates. |
| CSR | Certificate Signing Request |
| DMZ | Demilitarized Zone |
| 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 Publication |
| GDPR | General Data Protection Regulation |
| GLONASS | Global Navigation Satellite System |
| GPS | Global Positioning System |
| HSM | Hardware Security Module |
| HTTP | Hypertext Transfer Protocol |
| IEC | International Electrotechnical Commission |

| | |
|------------|--|
| IETF | Internet Engineering Task Force |
| INRIM | Italian National Institute of Metrological Research |
| 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. |
| MPLS | Multiprotocol Label Switching |
| NAS | Network-Attached Storage |
| 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 |
| OCSP | Online Certificate Status Protocol. Protocol for accessing the status of certificates. |
| OID | Object Identifier |
| OTP | One-time password |
| 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-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 |
| RFC | IETF Request for Comments |
| RSA | Rivest-Shamir-Adleman (type of public key algorithm) |
| RTO/RPO | Recovery Time Objective / Recovery Point Objective |
| SHA | Secure Hash Algorithm |
| SSL | Secure Sockets Layer (secure communication protocol) |
| STS | Station-to-Station protocol |
| TLS | Transport Layer Security (secure communication protocol that replaces SSL) |
| TS | Technical Specification |
| TSL | Trust-service Status List |
| TSP | Trust Service Provider |
| UPS | Uninterruptible Power Supply |
| 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 and the corresponding certificate profiles on the website at the following addresses:

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

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 under this CPS and the access addresses of their corresponding OCSP services 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.

The OCSP service of a CA under this CPS will no longer be available at its access address in the event of termination of the CA for a reason other than the compromise of its private key or in the event

of cessation of Camerfirma's activity as a TSP.

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 ON 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.
- 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.
- For CA and OCSP certificates (issued to legal persons), in the DN in the *Subject* field:
 - Descriptive name of the CA 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*).

Camerfirma publishes the datasheets of certificate profiles under these CPS and CPs on the website <https://policy2021.camerfirma.com>.

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 ANONYMITY OR PSEUDONYMITY OF SUBSCRIBERS

Under these CPs, Subjects are not permitted to use pseudonyms.

3.1.4 RULES FOR INTERPRETING VARIOUS NAME FORMS

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 ROLE OF TRADEMARKS

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

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

- In QSCD SmartCard/Token: the keys can be delivered by Camerfirma to the Subject/Signatory, directly or through a RA on a qualified signature creation device (QSCD).
- In QSCD Cloud: Camerfirma uses a remote key storage system, allowing the Subject/Signatory to access the private key from different devices. The keys are stored in an HSM QSCD, which allows the Subject/Signatory to use the private key under his/her sole control, and that complies with the requirements set out in Annex II of the eIDAS Regulation.

3.2.2 AUTHENTICATION OF ORGANIZATION IDENTITY

3.2.2.1 IDENTITY

Before the issuance of a certificate to a natural person with the attribute 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 used for identification of the Entities in Spain are:

- *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 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 Applicant's identity 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* or Passport.

Foreigners from UE or EEA with NIE:

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

Foreigners from UE or EEA with NIE:

- Passport or identity document issued by UE or EEA country and *Certificado de Número de Identificación Fiscal* (NIF).

Foreigners from UE or EEA without NIE or NIF:

- Passport or identity document issued by UE or EEA.

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 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 the national level which provide equivalent assurance in terms of reliability to physical presence, by the applicable regulation, in particular the conditions and technical requirements established in Orden ETD / 465/2021, of May 6, which regulates remote video identification methods for the issuance of qualified electronic certificates. The identification of the Applicant may be carried out in an assisted way, with the synchronous mediation of an operator, or in an unassisted way, without online interaction between an operator and the Applicant, but with a subsequent revision by an operator.

Camerfirma makes available to its users, various remote identification processes by video, which may be used to issue qualified electronic certificates, as long as they comply with the conditions and technical requirements required by the applicable regulation, which must be confirmed in 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, but with subsequent revision by an operator.

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

- If the Applicant has submitted a DNI or holds an NIE, Camerfirma must consult the Applicant's identity data through the intermediation platform of the Data Verification and Consultation Service that the control 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.

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 WITH THE ENTITY

| Certificate type | Documentation |
|--|--|
| Qualified Corporate Certificate | Usually, authorization signed by an Entity's legal representative. |
| Qualified Certificate for a Legal Representative of a Legal Entity | Documentation accrediting Entity's representation powers, depending on the type of representative and on the type of Entity. |
| Qualified Certificate for a Legal Representative of a Non-Legal Entity | |
| Qualified Certificate for a Voluntary Representative of a Legal Entity before the Public Administrations | |
| Qualified Certificate for a Voluntary Representative of a Non-Legal Entity before the Public Administrations | |
| Qualified Certificate for a Special Representative of a Legal Entity | |
| Qualified Certificate for a Special Representative of a Non-Legal Entity | |

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

According to article 24.2.h) of the eIDAS Regulation, this registration activity may be carried out by electronic means, both if the documents provided are valid electronic documents as well as paper documents. In the latter case, the Registry Operator must keep a scanned copy and digitally sign it with his/her certificate, 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

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

3.2.6 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 when its expiry date is close.

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

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.

The data of the Subject/Signatory in the certificate must not have changed and 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 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 its RAs, may, on its own initiative, request the revocation 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 InfoCert IPP (InfoCert Partner Platform) platform for lifecycle management for end entity certificates under these CPS and CPs.

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

The services of this platform 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 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

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

4.1.2 ENROLLMENT PROCESS AND RESPONSIBILITIES

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

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

- The Applicant is responsible for providing correct and truthful information on his identity and on specific attributes of the Subject, reading carefully the material made available by the CA – including through the RA – and following CA and/or RA instructions while submitting a qualified certificate application.
- The RA, if present, is responsible for – through the Registration Operator – the Applicant identification, and for the accuracy and validity of the attributes of the Subject/Signatory (in case of the certificate with attributes), informing them about the obligations derived from the certificate and following in detail the processes defined by the CA;
- The CA is ultimately responsible for Applicant identification, verification of attributes, and successful registration of the qualified certificate.

4.2 CERTIFICATE APPLICATION PROCESSING

To obtain a certificate for electronic signature, the Subject/Signatory, and the Subscriber if they are

different persons, must:

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

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

4.2.1 PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS

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

The CA may provide that the signature PIN is independently selected by the Applicant. In such cases, is the responsibility of the Applicant to remember the PIN.

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

4.2.2 APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS

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

4.2.3 TIME TO PROCESS CERTIFICATE APPLICATIONS

The applications submitted by the InfoCert IPP platform 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.

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

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

4.3 CERTIFICATE ISSUANCE

4.3.1 CA ACTIONS DURING CERTIFICATE ISSUANCE

4.3.1.1 CERTIFICATES ISSUED ON QSCD SMARTCARD/TOKEN

The RA generates the cryptographic key pair directly on a QSCD cryptographic smartcard or token using the applications supplied to it by the CA after secure authentication.

The RA sends the CA the digitally signed certificate request in PKCS #10 format, through a secure and authenticated channel.

After confirming that the signature on the PKCS #10 is authentic, the CA issues the certificate that is sent through the secure channel and stored in the cryptographic smartcard or token.

4.3.1.2 CERTIFICATES ON QSCD CLOUD (HSM)

The Subject/Signatory logs on to the RA services or applications.

The RA generates the cryptographic key pair directly on the HSM.

The RA sends the CA the digitally signed certificate request in PKCS #10 format through a secure and authenticated channel.

After confirming that the signature on the PKCS #10 is authentic, the CA issues the certificate that is stored in the HSM.

4.3.1.3 CERTIFICATES ISSUED FOR TESTING PURPOSES

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

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

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

actual certificate.

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

4.3.2 NOTIFICATION TO SUBSCRIBER BY THE CA OF ISSUANCE OF CERTIFICATE

If the certificate is issued on QSCD SmartCard/Token, the Subject/Signatory does not need to be notified of the certificate issuance as the certificate is stored in the device delivered to him.

If the certificate is issued on QSCD Cloud, the Subject/Signatory will receive the notification via the email address indicated at the time of registration.

4.3.3 ACTIVATION

4.3.3.1 ACTIVATION OF THE SIGNATURE DEVICE (SMARTCARD OR TOKEN)

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

4.3.3.2 ACTIVATION OF THE REMOTE SIGNATURE DEVICE (HSM)

After logging on to the CA website using the activation codes confidentially given to him, the Subject/Signatory selects a signature PIN, that is a confidential security parameter whose secrecy and protection are placed exclusively on the Subject/Signatory itself.

To confirm the PIN, the Subject/Signatory enters the One Time Password received via SMS.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE

Once the certificate has been delivered or notified, the Subject/Signatory has 14 days to verify that it has been issued correctly.

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

4.4.2 PUBLICATION OF THE CERTIFICATE BY THE CA

Once the certificate has been delivered or notified, it will be entered into the internal certificate registry and will not be made public by the CA.

4.4.3 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

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.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 SUBSCRIBER PRIVATE KEY AND CERTIFICATE USAGE

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

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

The key usage limitation is defined in the certificate content in the extensions: *Key Usage*, *Extended Key Usage* and *Basic Constraints*.

| CA | Key Usage | Extended Key Usage | Basic Constraints |
|--|--|-----------------------------|------------------------------|
| CAMERFIRMA ROOT 2021 | critical, cRLSign, keyCertSign | - | critical, CA:true |
| AC CAMERFIRMA QUALIFIED CERTIFICATES – 2021 | critical, cRLSign, keyCertSign | emailProtection, clientAuth | critical, CA:true, pathLen:0 |
| Qualified Citizen Certificate - QSCD SmartCard/Token, QSCD Cloud | critical, digitalSignature, contentCommitment, keyEncipherment | emailProtection, clientAuth | critical, CA:false |
| Qualified Corporate Certificate - | critical, | emailProtection, | critical, CA:false |

| | | | |
|---|--|-----------------------------|--------------------|
| QSCD SmartCard/Token, QSCD Cloud | digitalSignature, contentCommitment, keyEncipherment | clientAuth | |
| 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 |

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

4.5.2 THE 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, as well as of any representation powers and professional qualifications.

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 when its expiry date is close.

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:

- 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.
- No identification of the Applicant has ever been carried out in person.
- 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 only be requested by the Subject/Signatory,

4.7.3 PROCESSING CERTIFICATE RE-KEY REQUESTS

Certificate re-key is performed, using the key associated with the valid certificate to be re-keyed, through a specific service provided by the CA as part of its business and contractual relations with the Subject/Signatory and with the RA.

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 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 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 expiry date and time. Any signature created with it after its revocation becomes effective is invalidated.

The revocation of a certificate is definitive and therefore irreversible.

Under these CPS and CPs, certificate suspension is not allowed.

The revocation 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 certificates cannot be used under these CPS and CPs.

4.9.1 CIRCUMSTANCES FOR REVOCATION

Under this CPS, a certificate will be revoked due to:

As a general rule:

- 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 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.
- 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

Under this CPS, the request for the certificate revocation can be done 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 notify the RA or CA of 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.

The revocation will be requested via the online revocation service located on the following Camerfirma website, by entering the certificate revocation PIN and the value of the *dnQualifier* attribute in the DN in the *Subject* field of the certificate, 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, 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) 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.
- In the case of sending the request document to the CA, all types of end entity 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 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 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, as evidence of the revocation request.

- 3) 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.

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.

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.

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

This procedure is available for:

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

For end entity certificate revocation requests:

- An authorized operator (trusted role *Revocation Officers*) of the RA or the CA will request the revocation of the certificate on the certificate management platform Camerfirma STATUS®. The certificate may be revoked:
 - Individually, by selecting on the Camerfirma STATUS® platform the certificate to be revoked and, where applicable, the reason for revocation (it can be "unspecified"). The certificate revocation is performed immediately.
 - Together with other certificates, by uploading to the Camerfirma STATUS® platform 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 Camerfirma STATUS® platform, as evidence of the revocation 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 platform Camerfirma STATUS® (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 Camerfirma STATUS® platform, as evidence of the revocation request.

For revocation requests for Subordinate CA certificates and OCSP certificates:

- 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 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 external Subordinate CA certificates, once the request has been confirmed with the certificate Subscriber, the certificate will be revoked as follows:

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

The RA or the CA may request the immediate revocation of a certificate using procedure 4) 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) and 4) 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 revocation of the affected certificates using the aforementioned procedure 4), after having informed their respective Subscribers and Subjects.

4.9.4 REVOCATION REQUEST GRACE PERIOD

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

- Revocation of a Subordinate CA 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.

In these cases, the scheduled revocation date shall be considered 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, 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 and reports of events relating to revocation shall be processed on receipt.

In the case of procedures for revocation request with no subsequent participation of an operator (procedures 1) and 4) 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 2) and 3) 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. If the revocation request cannot be confirmed within this time, then the certificate status need not be changed.

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

The maximum delay between the processing of a revocation 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.

Therefore, if an RA or the CA decides to revoke a certificate, the CA shall register such revocation 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 THE 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 |
|---|---|----------|
| CAMERFIRMA ROOT 2021 | Maximum 1 hour after revocation / Maximum 365 days | 365 days |
| AC CAMERFIRMA QUALIFIED CERTIFICATES – 2021 | 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 |
|---|-----------------|
| CAMERFIRMA ROOT 2021 | 23 hours |
| AC CAMERFIRMA QUALIFIED CERTIFICATES – 2021 | Immediate |

4.9.9 ONLINE 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 ONLINE 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 for compromise of its private key (see section 5.7.3), with the *default* OCSP certificate (see section 1.3.1.2).
- 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 CA's OCSP service will no longer be available at its access address.
- 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 |
|---|-----------------|----------|
| CAMERFIRMA ROOT 2021 | 24 hours | 1 hour |
| AC CAMERFIRMA QUALIFIED CERTIFICATES – 2021 | 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.

The date of revocation of a Subordinate CA certificate shall be agreed in advance with the Subscriber (see section 4.9.4). When an external Subordinate CA certificate is revoked, an email notification

will be sent to the Subscriber specifying the date and time of revocation and the reason for the revocation.

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

Under these CPS and CPs, certificate suspension is not allowed.

4.9.14 WHO CAN REQUEST SUSPENSION

No stipulation.

4.9.15 PROCEDURE FOR SUSPENSION REQUEST

No stipulation.

4.9.16 LIMITS ON SUSPENSION PERIOD

No stipulation.

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 issues a single CRL.

Each Subordinate CA under this CPS issues one CRL for every 50,000 issued certificates.

CRLs issued by CAs under this CPS include revoked certificates that have expired, with no time limit after their expiry.

OCSP services 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, 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 the *default* OCSP certificate (see section 1.3.1.2) 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 be available at its access address.

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

4.12 KEY ESCROW AND RECOVERY

4.12.1 KEY ESCROW AND RECOVERY POLICY AND PRACTICES

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

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.

4.12.2 SESSION KEY ENCAPSULATION AND RECOVERY POLICY AND PRACTICES

No stipulation.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

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

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

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

5.1 PHYSICAL CONTROLS

The implemented measures provide adequate security on:

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

5.1.1 SITE LOCATION AND CONSTRUCTION

Camerfirma uses three facilities:

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

These facilities are located in:

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

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

- InfoCert Data Center is located in Padova, Italy. The Disaster Recovery site is in Modena and is connected to the above Data Center by a dedicated redundant connection on two separate MPLS 40 Gbit/s each circuit upgradable to 100 Gbit/s.

Within both sites, rooms protected with several physical and logical security systems have been created. Each room hosts the computer equipment that is at the core of the digital certification, time stamping, and remote/automatic signature services.

- For services that need business continuity with RTO/RPO values close to zero, some components of the CAs services relating to the publication of the CRLs and the OCSP are hosted on AWS cloud, respectively, in Frankfurt Europe Region and in Ireland Europe Region. AWS has certifications of conformity in accordance with the ISO/IEC 27001:2013, 27017:2015, 27018:2019, and ISO/IEC 9001:2015 standards.

5.1.2 PHYSICAL ACCESS

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

5.1.3 POWER AND AIR CONDITIONING

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

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

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

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

The power supply infrastructure includes:

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

Each technology cabinet installed at the Data Center is powered by two power lines that assure the

HA in case of an outage of one of the two available lines.

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

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

5.1.4 WATER EXPOSURES

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

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

5.1.5 FIRE PREVENTION AND PROTECTION

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

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

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

Each fire compartment has a dedicated fire extinguishing system.

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

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

5.1.6 MEDIA STORAGE

Each demountable storage device 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 authorization.

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

5.1.7 WASTE DISPOSAL

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

5.1.8 OFF-SITE BACKUP

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

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

5.2 PROCEDURAL CONTROLS

5.2.1 TRUSTED ROLES

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

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

5.2.3 IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE

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

Depending on the asset, resources are accessed via login/password, digital certificates, physical keys, or SmartCard or Token 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

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

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

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

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

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

In general, Camerfirma removes an employee's trust role 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 performed.
- Delinquency.

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

5.3.2 BACKGROUND CHECK PROCEDURES

Camerfirma Human Resource procedures include conducting relevant investigations before hiring anyone.

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

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

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

5.3.3 TRAINING REQUIREMENTS

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

Training includes the following content:

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

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

5.3.4 RETRAINING FREQUENCY AND REQUIREMENTS

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

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

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

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

5.3.5 JOB ROTATION FREQUENCY AND SEQUENCE

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

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

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

5.3.6 SANCTIONS FOR UNAUTHORIZED ACTIONS

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

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

5.3.7 INDEPENDENT CONTRACTOR REQUIREMENTS

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

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

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

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

5.3.8 DOCUMENTATION SUPPLIED TO PERSONNEL

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

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

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

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

5.4 AUDIT LOGGING PROCEDURES

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

5.4.1 TYPES OF EVENTS RECORDED

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

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

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

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

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

All logical accesses to the CA applications are recorded.

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

5.4.2 FREQUENCY OF PROCESSING LOG

Data collection, clustering, and archiving on the InfoCert preservation system occur monthly.

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

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

5.4.5 AUDIT LOG BACKUP PROCEDURES

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

5.4.6 AUDIT COLLECTION SYSTEM (INTERNAL VS. EXTERNAL)

Event logs are collected through ad hoc automatic procedures and archived in the InfoCert preservation system according to the methods described in the InfoCert preservation system security manual.

5.4.7 NOTIFICATION TO EVENT-CAUSING SUBJECT

No stipulation.

5.4.8 VULNERABILITY ASSESSMENTS

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

5.5 RECORDS ARCHIVAL

5.5.1 TYPES OF RECORDS ARCHIVED

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

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

5.5.2 RETENTION PERIOD FOR ARCHIVE

The CAs preserve the documentation detailed in section 5.5.1 for at least 15 years after the expiration date of any certificate issued based on that documentation.

5.5.3 PROTECTION OF ARCHIVE

Protection is ensured by the InfoCert preservation system, accredited by AgID.

5.5.4 ARCHIVE BACKUP PROCEDURES

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

5.5.5 REQUIREMENTS FOR TIME-STAMPING OF RECORDS

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

5.5.6 ARCHIVE COLLECTION SYSTEM (INTERNAL OR EXTERNAL)

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

5.5.7 PROCEDURES TO OBTAIN AND VERIFY ARCHIVE INFORMATION

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

5.6 KEY CHANGEOVER

The 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.

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

5.7.1 INCIDENT AND COMPROMISE HANDLING PROCEDURES

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

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

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

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

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

5.7.3 ENTITY PRIVATE KEY COMPROMISE PROCEDURES

A CA, Root or 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 the 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, InfoCert and 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 communication on the Camerfirma website.
- Indicate in the above information:
 - Date and time of becoming aware of the compromise of the CA's private key.
 - 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 the *default* OCSP certificate issued by another CA (see section 1.3.1.2).

When Camerfirma is informed of the compromise of the private key of any external Subordinate CA within the hierarchies under this CPS, it shall revoke the certificate/s associated with the compromised private key and shall consider the CA as terminated (see section 5.8.2).

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 and InfoCert have adopted the procedures required to ensure continuity of their 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 a TSP issuing qualified certificates.
- 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 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.

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 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 Parts.
- 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 OCSP service shall no longer be available at its access address.

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 the *default* OCSP certificate (see section 1.3.1.2).

- 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.

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

To provide its service, the CA needs to generate a key pair used to sign the end entity certificates.

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

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

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

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

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

| CA | Key length | Signature algorithm | Creation | Expiry |
|---|------------|-------------------------|------------|------------|
| 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 |

6.1.1.1 CREATING THE SUBJECT'S KEY PAIR

Asymmetric keys are generated within a device QSCD provided by Camerfirma using native features provided by the devices themselves.

The keys have a minimum length of 2.048 bits.

6.1.1.2 KEY CREATION HARDWARE/SOFTWARE

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

The Root CA and Subordinate CAs keys use a cryptographic device that complies with FIPS-104-2 level 3 or CC EAL 4 or CC EAL 4 or higher specifications.

6.1.2 PRIVATE KEY DELIVERY TO THE SUBSCRIBER

Private keys are contained in the device QSCD.

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

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

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

6.1.3 PUBLIC KEY DELIVERY TO THE 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 THE RELYING PARTIES

See section 2.2.3.

6.1.5 KEY SIZES

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

The Root CA and Subordinate CAs keys can be:

- RSA asymmetric keys with a length of not less than 4096 bits;
- EC asymmetric keys on one of the elliptic curves provided by ETSI document TS 119 312 – Cryptographic Suites with a length of not less than 256 bits.

See section 6.1.1 for the key length of Root and Subordinate CA certificates active in the hierarchies under this CPS.

The end entity certificate keys may be:

- RSA asymmetric keys with a length of not less than 2048 bits;
- EC asymmetric keys on one of the elliptic curves provided by ETSI TS 119 312 – Cryptographic Suites document with a length not less than 256 bits.

6.1.6 PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING

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

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

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

Cryptographic modules used by Camerfirma for certification keys (CA) and OCSP server are certified FIPS 140 Level 3 or CC EAL 4 or higher.

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

QSCD Cloud devices are certified FIPS 140 Level 3 and/or CC EAL 4+.

Camerfirma shall check compliance of used QSCD SmartCard/Token devices and QSCD Cloud 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. If Camerfirma detects in these checks that any of these devices is not considered a QSCD anymore, Camerfirma shall revoke all active certificates in which the private key is in that device.

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

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

6.2.3 PRIVATE KEY ESCROW

No stipulation.

6.2.4 PRIVATE KEY BACKUP

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

6.2.5 PRIVATE KEY ARCHIVAL

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

6.2.6 PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE

No stipulation.

6.2.7 PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE

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

6.2.8 METHOD OF ACTIVATING PRIVATE KEY

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

The Subject is responsible for protecting his private key with a strong password to prevent unauthorized use. To activate the private key, the Subject must authenticate himself.

6.2.9 METHOD OF DEACTIVATING PRIVATE KEY

No stipulation.

6.2.10 METHOD OF DESTROYING PRIVATE KEY

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

The CA's private key shall be securely deleted from the 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.

6.2.11 CRYPTOGRAPHIC MODULE RATING

No stipulation.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 PUBLIC KEY ARCHIVAL

No stipulation.

6.3.2 CERTIFICATE OPERATIONAL PERIODS AND KEY PAIR USAGE PERIODS

A certificate validity period shall be determined based on:

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

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 1.3.1.2): 1 year.
- Qualified certificates issued by Camerfirma Subordinate CAs: not more than 5 years.

6.4 ACTIVATION DATA

See sections 4.3.3 and 6.3.

6.5 COMPUTER SECURITY CONTROLS

Camerfirma and InfoCert use reliable systems to provide certification services. Camerfirma and InfoCert have undertaken IT controls and audits to manage their IT assets with the security level required for managing digital certification systems.

Regarding information security, the certification model on ISO 270001 information management systems is followed.

6.5.1 SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS

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

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

6.5.2 COMPUTER SECURITY RATING

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

6.6 LIFE CYCLE TECHNICAL CONTROLS

The certificates store the Subject's keys in a qualified signature creation device (Hardware). The hardware device is a cryptographic SmartCard or Token certified as a qualified signature creation device in compliance with Appendix II of eIDAS.

As regards hardware devices:

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

- The device can be reused and can store several key pairs securely.
- The device is owned by the Subject.

Concerning the devices used in the *Cloud QSCD* management: the device that stores these keys are FIPS-104-2 level 3 or CC EAL 4+ certified and authorized by the Supervisory Body for services catalogued as *QSCDManagedOnBehalf*.

6.6.1 SYSTEM DEVELOPMENT CONTROLS

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

6.6.2 SECURITY MANAGEMENT CONTROLS

6.6.2.1 SECURITY MANAGEMENT

Camerfirma 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 the level of confidentiality.

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

6.6.2.3 MANAGEMENT PROCEDURES

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

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

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

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

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

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

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

6.6.2.4 ACCESS SYSTEM MANAGEMENT

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

- There are controls based on firewalls, antivirus, and IDS with high availability.
- Sensitive data is protected via cryptographic methods or strict identification access controls.
- Camerfirma has established a documented procedure to process user registrations and cancellations and a detailed access policy in its security policy.
- Camerfirma has implemented procedures to ensure tasks are undertaken in accordance with the roles policy.
- Each person is assigned a role to carry out certification procedures.
- Camerfirma employees are responsible for their actions in accordance with the confidentiality agreement signed with the company.
- Creating the certificate: Authentication for the issuance process is via an m out of n operators system to activate the CA's private key.
- Revocation management: Revocation takes place via strict SmartCard or Token based authentication of an 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.

6.6.2.5 MANAGING THE CRYPTOGRAPHIC HARDWARE LIFECYCLE

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

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

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

At least two trusted employees are required 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

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

Camerfirma and InfoCert systems and networks are connected to the Internet in a controlled way using firewall systems that allow splitting up the connection into progressively more secure areas: Internet networks, DMZ (Demilitarized Zone), or Perimeter Networks, and Internal networks. All traffic flowing between areas is subject to acceptance by the firewall, based on a set of established rules. Firewall rules are designed based on "default deny" (what is not expressly permitted is forbidden by default, or the rules will only allow what is strictly necessary for the application to properly work) and "defense in depth" (increasing layers of defense are arranged, first at the network level, through successive firewall barriers, and finally at the system level through hardening) principles.

6.8 TIME-STAMPING

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

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

Certificate profiles 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://policy2021.camerfirma.com>.

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:

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

The public key algorithm OID in *Subject Public Key Info* field is:

- 1.2.840.113549.1.1.1 - *rsaEncryption*

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.

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 and OCSP 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 and 1.3.1.2.

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

7.2 CRL PROFILE

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, including only the *keyIdentifier* field.

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 issued by the Subordinate CA AC CAMERFIRMA QUALIFIED CERTIFICATES - 2021 include both extensions.

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

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

Camerfirma performs an internal audit on entities that have obtained a Subordinate CA certificate and that issue and manage certificates with their own technical and operational resources. It can be replaced by a favorable report of the corresponding ETSI regulations such as ETSI EN 319 411-1 or the applicable regulations in the country where the Subordinate operates.

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

Through its auditors, Camerfirma conducts an annual audit on the Entities that have obtained a Subordinate CA certificate and that issue certificates with their own operational resources, from infrastructures technically controlled by Camerfirma. This audit can be replaced by a favorable ETSI standard report corresponding to certificates issued as ETSI EN 319 411-1.

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 THE 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.
- Camerfirma Perú complies with Peruvian regulation and INDECOPI Guidelines.

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.

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

9.1.2 CERTIFICATE ACCESS FEES

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

9.1.3 REVOCATION OR STATUS INFORMATION ACCESS FEES

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

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://policy2021.camerfirma.com>.

9.1.5 REFUND POLICY

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

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

9.2 FINANCIAL RESPONSIBILITY

9.2.1 INSURANCE COVERAGE

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

9.2.2 OTHER ASSETS

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

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

Camerfirma complies with current legislation on personal data protection:

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

9.3.2 INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION

Camerfirma deems the following information not confidential:

- The contents of this CPS and CP.
- The information included in the certificates, CRLs, and OCSP responses.
- Any information whose accessibility is prohibited by current law.

9.3.3 RESPONSIBILITY TO PROTECT CONFIDENTIAL INFORMATION

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

For end entities certificates, the Subject or the Person Responsible are responsible to protect their private key and all activation information (i.e. passwords or PIN) needed to access or use the private key.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 PRIVACY PLAN

In any case, Camerfirma complies with current regulations regarding data protection, in particular, it has adapted its procedures to the EU Regulation 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 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 data controller to adequately protect private information.

9.4.5 NOTICE AND CONSENT TO USE PRIVATE INFORMATION

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

9.4.6 DISCLOSURE PURSUANT TO JUDICIAL OR ADMINISTRATIVE PROCESS

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

9.4.7 OTHER INFORMATION DISCLOSURE CIRCUMSTANCES

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

9.5 INTELLECTUAL PROPERTY RIGHTS

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

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 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.
- Revoke certificates in accordance with these CPS and CPs and publish the revocations in CRLs and OCSP services.

- Inform Subjects about the revocation 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 when it is legally provided for or allowed to be stored or copied.
- If the CA (or, when applicable, another QTSP) generates the Subject's keys, generate (or, when applicable, confirm that another QTSP 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) generates the Subject's keys, use (or, when applicable, confirm that another QTSP 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 QSCD SmartCard/Token, generate the keys within the secure cryptographic device QSCD SmartCard/Token.
- For certificates issued on QSCD Cloud devices managed by the CA (or, when applicable, by another QTSP) generate in a QSCD HSM and keep (or, when applicable, confirm that another QTSP generates in an QSCD HSM and keeps) with due diligence the private keys of the certificates, ensuring that they can only be used within an QSCD HSM 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 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 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 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

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

- Protect their private keys.
- Issue certificates pursuant to the corresponding CPS and CPs and applicable regulations in force.
- Issue certificates that are free from errors.

- Respect in any case the provisions on the protection of personal data in the regulations in force.
- Allow, if applicable, an annual audit by Camerfirma.
- Safeguard, for the duration established by law, the documentary information and systems that have been used or generated for issuing certificates.
- Notify Camerfirma of any incident in the delegated activity.

Responsibility of the external Subordinate CAs:

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

9.6.2 RA REPRESENTATIONS AND WARRANTIES

RAs are entities that the CAs appoint 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 this CPS and CP for issuing certificates and in accordance with current law, particularly to:

- Adhere to the provisions of this CPS, CP applicable to each kind of issued certificate and applicable regulations in force.
- Protect their private keys that are used for exercising their functions.
- Respect the terms of the agreement signed with the CA.
- Respect the Terms and Conditions accepted by the Subject and, where applicable, the Subscriber.
- Respect in any case the provisions on the protection of personal data in the regulations in force.

Regarding the life cycle of certificates:

- Before the issuance of the certificate:
 - Check the identity of the Subject/Signatory and, where applicable, the Subscriber of a certificate according to the methods defined in these CPS and CPs.
 - Check the accuracy and authenticity of the information provided by the Applicant and, where applicable, the Subscriber.
 - Inform the Subject/Signatory and, where applicable, the Subscriber about his/her obligations, about the way to use the certificate and, if applicable the cryptographic device, and data to accede to them, and about the process he/she has to follow in case of misuse or lost the certificate or device, limits of use, liability, etc. and where he/she can access to consult CPS, CPs and Terms and Conditions.

- Provide the Subject/Signatory and, where applicable, the Subscriber with the certificate according to these CPS and CPs.
- If applicable, deliver the corresponding cryptographic device to the Subject/Signatory.
- Formalize the Terms and Conditions and other contractual documents with the Subject/Signatory and, where applicable, the in an analogic manner or using digital tools that enable the conservation of the formal acceptance.
- After the issuance:
 - Keep the documents provided by the Subject and/or the Subscriber and signed Terms and Conditions in a physical or digital archive file for the period required by current law.
 - 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.

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

In the event of a claim from a Subject/Signatory, a Subscriber, an Entity or a Relying Party, the CAs must offer proof that it has acted diligently and if there is evidence that the cause of the claim is due to incorrect data validation or checking, the CAs can hold the RAs liable for the consequences, in accordance with the agreement signed with the RAs.

To avoid breaches of RA's obligations, the CAs control periodically the RAs activity and audit at least each two (2) years the resources used and their knowledge and control over the operational procedures used to provide the RA services.

The same responsibilities are assumed by the RAs in virtue of breaches of the delegated entities such as Points of Physical Verification (PPV) and Points of Remote Verification (PRV), where applicable, 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 Entity.
- Where applicable, provide the RA with required information and/or documentation of the Applicant, 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 Entity.
- Where applicable, provide the RA with required information and/or documentation of the Applicant, 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.

9.6.3.3 SUBJECT AND PERSON RESPONSIBLE

The Subject, and at the same time the Person Responsible, 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.
- 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 revocation of the certificate, or once the term of validity of the certificate has expired.
- Make use of the certificate as personal and non-transferable and custody of the private key activation data in a diligent manner. Subject/Signatory will be solely responsible to Relying Party and, if applicable, to Entity he/she represents in case of not having authorization, and for the consequences, if misused or not properly controlled.
- Authorize the CA and 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 fulfill 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 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 QSCD SmartCard/Token device, in order to avoid unauthorized use.
- In the case of certificates in a QSCD SmartCard/Token device, if it loses its possession, make it known to the RA or the CA as soon as possible and, in any case, within 24 hours following the production of the aforementioned circumstance, regardless of the specific event that originated it or the actions that it may eventually exercise.
- Not to use the private key, the electronic certificate, or any other technical support provided by the CA or RA to carry out any transaction prohibited by the applicable law.

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 Entity.

- Where applicable, provide the RA with required information and/or documentation of the Applicant, 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 Relying 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 RAs 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.
- 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 about allowed use and a 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 included in the certificate if these data have been evidenced through a public document registered in a public register if required.
- An inadequate or fraudulent use of the certificate in case the Subject and/or, if applicable, the Person Responsible has transferred it or authorized its use in favour of a third person being the sole responsibility of the Subject and, if applicable, the Person Responsible the control of the keys associated with the 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 the certificates, CRLs or OCSP responses.
- Damages caused during verification of the causes for revocation.
- Due to the content of messages or documents signed or encrypted digitally.
- Failure to retrieve encrypted documents with the Subject's public key.

9.8 LIMITATIONS OF LIABILITY

9.8.1 CA LIMITATIONS OF LIABILITY

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

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

The CA shall be liable for any damage caused to the Subscriber or the Subject or any Relying Party, provided there is fraud or major negligence, about:

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

9.8.2 RA LIMITATIONS OF LIABILITY

The RA shall be fully responsible for the identification and authentication procedure of Subscribers, Applicants, Subjects, Persons Responsible and Entities. It shall do so in accordance with the provisions of these CPS and CPs.

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

9.8.3 SUBSCRIBER, APPLICANT, SUBJECT, PERSON RESPONSIBLE AND ENTITY LIMITATIONS OF LIABILITY

It is the full liability of the Subscriber, the Applicant, the Subject, the Person Responsible and the Entity to comply with the obligations stipulated in these CPS and CPs and in legal documents signed by them.

9.8.4 CAMERFIRMA LIMITATIONS OF LIABILITY

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

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

9.9 INDEMNITIES

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

9.10 TERM AND TERMINATION

9.10.1 TERM

See section 5.8.

9.10.2 TERMINATION

See section 5.8.

9.10.3 EFFECT OF TERMINATION AND SURVIVAL

See section 5.8.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

Any notification about this CPS shall be made by email or certified mail to any of the addresses listed in section 1.5.2.

9.12 AMENDMENTS

9.12.1 PROCEDURE FOR AMENDMENT

Camerfirma reserves the right to modify this document for technical reasons or to reflect any changes in the procedures that have occurred due to legal, and regulatory requirements (eIDAS Regulation, CA/B Forum, National Supervisory Bodies, etc.) or as a result of the optimization of the work cycle. Each new version of this document replaces all previous versions, which remain, however, applicable to the certificates issued while those versions were in force. At least one annual update will be published. These updates will be reflected in the version document history at the end of the document.

Changes that can be made to this document do not require notification except that it directly affects the rights of the Subscribers or the Subjects/Signatories, in which case they may be notified within 15 days through the Camerfirma web page.

9.12.2 NOTIFICATION MECHANISM AND PERIOD

9.12.2.1 *LIST OF ASPECTS*

Any aspect of this document can be changed without notice.

9.12.2.2 *NOTIFICATION METHOD*

Any proposed changes to this document are published immediately on Camerfirma's website <https://policy2021.camerfirma.com>

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

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

9.12.2.3 *PERIOD FOR COMMENTS*

The affected Subscribers and Subjects/Signatories can submit their comments to the policy management organization within 15 days following receipt of the 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

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

9.14 GOVERNING LAW

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

9.15 COMPLIANCE WITH APPLICABLE LAW

See section 9.14.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 ENTIRE AGREEMENT

Parties to this 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 individual provisions of this CPS prove to be ineffective or incomplete, this shall be without prejudice to the effectiveness of all other provisions.

The ineffective provision will be replaced by an effective provision deemed as most closely reflecting the sense and purpose of the ineffective provision. In the case of incomplete provisions, amendment will be agreed as deemed to correspond to what would have reasonably been agreed upon in line with the sense and purposes of this CPS, had the matter been considered beforehand.

9.16.4 ENFORCEMENT (ATTORNEYS' FEES AND WAIVER OF RIGHTS)

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

9.17 OTHER PROVISIONS

No stipulation.

Appendix I: Document history

| | | |
|------------|--------|--|
| 19/01/2022 | V1.0.0 | Initial version |
| 31/03/2023 | V1.1.0 | <p>The document format is updated and a document code is added.</p> <p>New CPs Qualified Citizen Certificate are added.</p> <p>Revision and homogenization of terms and acronyms.</p> <p>Correction of CPS and CPs location.</p> <p>1.1. Revision</p> <p>1.2. Review and update. New CPs Qualified Citizen Certificate are added.</p> <p>1.3 and all its sections. Revision and update.</p> <p>1.3.1.1. The scope of the hierarchy is changed so that CAs and RAs have no territorial limitations. All the CAs that operate under this hierarchy do so from infrastructures technically controlled by Camerfirma.</p> <p>1.3.1.1. New CPs Qualified Citizen Certificate.</p> <p>1.3.1.2 OCSP certificates. New section.</p> <p>1.3.2 RA. Nuevo PRV (Point of Remote Verification).</p> <p>1.3.3 Subscribers. Sections formerly in 1.3.1 Other participants are incorporated. Changes in names of participants.</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 its sections. Review and update. Removal of section 3.2.5.3.</p> <p>3.2.3. The assisted process with pre-validation of documentation and synchronous mediation by an operator is removed as a remote video identification process.</p> <p>4.4.3. Notification to other entities of OCSP certificates and Subordinate CAs is added.</p> <p>4.5.1. Update of CPs. New PCs Qualified Citizen Certificate.</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. New online revocation procedure. The procedure for revocation request made by the RA or the CA is described. New procedure for reports of events</p> |

| | | |
|--|--|--|
| | | <p>which may indicate the need to revoke certificates.</p> <p>4.9.4 Examples of specific cases that require a future revocation date are explained.</p> <p>4.9.11. Revocation notifications sent to the end entity certificate Subject and to the Subscriber of Subordinate CA and TSU certificates are described.</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>4.12. New sections 4.12.1 and 4.12.2 with key custody and recovery policy and practices.</p> <p>5.2.1. 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. Table with CA keys data is added.</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>7 and its sections. Revision and update.</p> <p>8 and its sections. Revision and update.</p> <p>8, 8.1, 8.2. The audits that are performed are indicated.</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> |
|--|--|--|

| | | |
|--|--|---|
| | | 9.17 Other provisions. New section with "No stipulation" content. Other minor changes and corrections. |
|--|--|---|