firmaprofesional

Qualified Service Policy

Statement of Practices and Remote Qualified Electronic Signature Service Policy (SPPS) of Firmaprofesional, S.A.

Version: 240801

Classification: Public

BARCELONA
PASSEIG DE GRÀCIA 50, 2-1
08007 BARCELONA
+34 934 774 245

MADRID
CALLE CANTABRIA 5 (Ed. Amura)
28108 ALCOBENDAS
+34 915 762 181

WWW.FIRMAPROFESIONAL.COM

Version history

Version	Section and changes	Date of publication
220308	• Creation of the document	08/03/2022
230216	• Annual Review	16/02/2023
230413	• Update section 4.3.1	13/04/2023
240520	• Update section 1.1 • Update of the location of the entity on the main page • Changes related with the classification of the documentation	20/05//2024
240801	• Update of sections 1.1, 4.3.1.1, 4.3.1.4, 4.5.1.1, and 6.1 to include new hardware	01/08/2024

Index

1. Introduction 11
1.1. Summary 11
1.2. Identification of the Document 12
1.3 Participating Entities 12
1.3.1. Certification Authorities (CA) 12
1.3.2 Registration Authorities (RA) 12
1.3.3 Subscribers 13
1.3.4. Third parties trusting in certificates 15
1.3.5 Other participants 15
1.4. Certificates use 16
1.4.1. Appropriate use of certificates 16
1.4.2. Non authorized use of certificates 17
1.5 Policy Administration 17
1.5.1 Organization managing the document 17
1.5.2 Contact person 17
1.5.3 Person who determines the suitability of the CP for the policy 17
1.5.4 CP approval procedure 18
1.6 Definitions and acronyms 18
2. Repositories and Publication of Information 18
2.1 Repositories 18
2.2 Publication of certification information 18
2.3 Time or frequency of publication 18
2.4 Repositories access control 18
3. Identification and Authentication 19
3.1 Registration of Names 19
3.1.1 Types of names 19

3.1.2 Need for names to be meaningful 19
3.1.3 Anonymity or pseudonymity of subscribers 19
3.1.4 Rules for interpreting various forms of names 19
3.1.5 Uniqueness of names 19
3.1.6 Recognition, Authentication and Role of Trademarks 20
3.2 Initial validation of identity 20
3.2.1 Private key possession test method 20
3.2.2 Authentication of the organization's identity and domain identity 20
3.2.3 Authentication of the identity of a natural person 20
3.2.4 Unverified subscriber information 20
3.2.5 Validation of the identity of the RA and its operators 20
3.2.6 Interoperability criteria 20
3.3 Identification and authentication for key renewal requests 21
3.3.1 Identification and authentication for password change 21
3.3.2 Identification and authentication for the renewal of certificates after their revocation 21
3.4 Identification and authentication for revocation request 21
4. Certificate life cycle operational requirements 21
4.1. Application 21
4.1.1 Who can submit a certificate request 21
4.1.2 Certificate application process and responsibilities 21
4.2 Processing of certificate applications 22
4.2.1 Performing identification and authentication functions 22
4.2.2 Approval or denial of certificate applications 22
4.2.3 Processing time for certificate requests 22
4.3 Certificate issuance and Initialization of the signing keys 22
4.3.1 Actions of the CA during the issuance of the certificate 23
4.3.2 Notification to the subscriber by the CA of the issuance of the certificate and delivery 25

4.4 Certificate acceptance 25
4.4.1 Form in which the certificate is accepted 25
4.4.2 Certificate publication by the CA 26
4.4.3 Notification of the issuance of the certificate by the CA to other entities 26
4.5 Use of keys and certificate 26
4.5.1 Use of the subscriber's certificate and private key 26
4.5.2 Use of Trusting Party Certificates and Public Keys 29
4.6 Renewal of the certificate (without change of keys) 29
4.6.1 Circumstance for certificate renewal 29
4.6.2 Who can request renewal 29
4.6.3 Processing certificate renewal requests 29
4.6.4 Notification to the subscriber of the issuance of a new certificate 30
4.6.5 Conduct that constitutes acceptance of a renewal certificate 30
4.6.6 Publication of the renewal certificate by the CA 30
4.6.7 Notification of the issuance of the certificate by the CA to other entities 30
4.7 Certificate renewal with password change 30
4.7.1 Circumstance for changing the certificate key 30
4.7.2 Who can request the certification of a new public key 30
4.7.3 Processing certificate key change requests 31
4.7.4 Notification to the subscriber of the issuance of a new certificate 31
4.7.5 Conduct that constitutes acceptance of a certificate with a new key 31
4.7.6 Publication of the certificate with a new key by the CA 31
4.8 Modification of the certificate 31
4.8.1 Circumstance for the modification of the certificate 31
4.8.2 Who can request the modification of the certificate 31
4.8.3 Processing certificate modification requests 32
4.8.4 Notification to the subscriber of the issuance of a new certificate 32
4.8.5 Conduct that constitutes acceptance of the modified certificate 32
4.8.6 Publication of the certificate modified by the CA 32

4.8.7 Notification of the issuance of the certificate by the CA to other entities 32
4.9 Revocation and suspension of certificates 32
4.9.1 Circumstances for revocation 32
4.9.2 Who can request revocation 32
4.9.3 Revocation request procedure 33
4.9.4 Grace period for revocation request 33
4.9.5 Time within which CA must process the revocation request 33
4.9.6 Revocation verification requirement for relying parties 33
4.9.7 CRL emission frequency 33
4.9.8 Maximum latency for CRLs 33
4.9.9 Online Revocation / Status Check Availability 33
4.9.10 Online revocation verification requirements 34
4.9.11 Other forms of revocation announcements available 34
4.9.12 Special requirements related to the key engagement 34
4.9.13 Circumstances for suspension 34
4.9.14 Who can request suspension 34
4.9.15 Suspension request procedure 34
4.9.16 Limits of the suspension period 34
4.10 Certificate status services 35
4.10.1 Operational characteristics 35
4.10.2 Service availability 35
4.10.3 Optional functions 35
4.11 Termination of subscription 35
4.12 Custody and recovery of keys 35
4.12.1 Key custody and recovery policy and practices 35
4.12.2 Session Key Encapsulation and Recovery Policy and Practices 35
5. Physical security, facilities, management and operational controls 36
5.1 Physical controls 36
5.1.1 Site location and construction 36

5.1.2 Physical access 36
5.1.3 Energy and air conditioning 36
5.1.4 Exposure to water 36
5.1.5 Fire prevention and protection 36
5.1.6 Media storage 37
5.1.7 Waste disposal 37
5.1.8 Off-site backup 37
5.2 Procedural controls 37
5.2.1 Trusted roles 37
5.2.2 Number of people needed per task 38
5.2.3 Identification and authentication for each role 38
5.2.4 Roles requiring separation of duties 38
5.3 Personnel controls 38
5.3.1 Qualifications, experience and authorization requirements 38
5.3.2 Background check procedures 38
5.3.3 Training requirements 38
5.3.4 Frequency and requirements of retraining 39
5.3.5 Frequency and sequence of job rotation 39
5.3.6 Sanctions for unauthorized actions 39
5.3.7 Requirements for independent contractors 39
5.3.8 Documentation provided to personnel 39
5.4 Audit log procedures 39
5.5 Log file 40
5.6 Password change 41
5.7 Disaster recovery plan 41
5.8 Cessation of activity of the RA or CA 41
6. Technical security controls 41
6.1 Key pair generation and installation 41
6.2 Private key protection and cryptographic module engineering controls 41

6.3 Other aspects of key pair management 42
6.4 Activation data 42
6.5 IT security controls 42
6.6 Technical life cycle controls 42
6.7 Network security controls 42
6.8 Time control 43
7. Profiles of certificates, CRL and OCSP 43
7.1 Certificate profile 43
7.1.1 Version number 43
7.1.2 Certificate extensions 43
7.1.3 Algorithm object identifiers 43
7.1.4 Name forms 43
7.1.5 Name restrictions 44
7.1.6 Certificate policy object identifier 44
7.1.7 Using the Policy Constraints extension 45
7.1.8 Syntax and semantics of policy qualifiers 45
7.1.9 Processing semantics of the critical Certificate Policies extension 45
7.2 CRL profile 45
7.2.1 Version number 45
7.2.2 CRL extensions and CRL entries 45
7.3 OCSP profile 46
7.3.1 Version number 46
7.3.2 OCSP extensions 46
8. Compliance audits and other controls 46
8.1 Frequency of audits 46
8.2 Qualification of the auditor or evaluator 46
8.3 Relationship between the auditor and the audited authority 46
8.4 Aspects covered by the evaluation 46
8.5 Actions to be taken as a result of the detection of deficiencies 47

9. Other legal and business issues 47
9.1. Rates 47
9.1.1 Certificate issuance or renewal fees 47
9.1.2 Certificates access fees 47
9.1.3 Revocation or status information access fees 47
9.1.4 Fees for other services 48
9.1.5 Reimbursement fees 48
9.2 Financial responsibilities 48
9.2.1 Insurance coverage 48
9.2.2 Other assets 48
9.2.3 Insurance or guarantee coverage for end entities 48
9.3 Confidentiality of commercial information 48
9.3.1 Scope of confidential information 48
9.3.2 Non-confidential information 49
9.3.3 Responsibility to protect confidential information 49
9.4 Protection of personal information 49
9.4.1 Personal data protection policy 49
9.4.2 Information treated as private 49
9.4.3 Information not considered private 49
9.4.4 Responsibility to protect private information 49
9.4.5 Notice and consent to the use of private information 50
9.4.6 Disclosure under judicial or administrative process 50
9.4.7 Other information disclosure circumstances 50
9.5 Intellectual property rights 50
9.6 Obligations and guarantees 50
9.6.1 Obligations of the CA 50
9.6.2 Obligations of the RA 50
9.6.3 Obligations of applicants 51
9.6.4 Representations and guarantees of third parties who trust the certificates 51

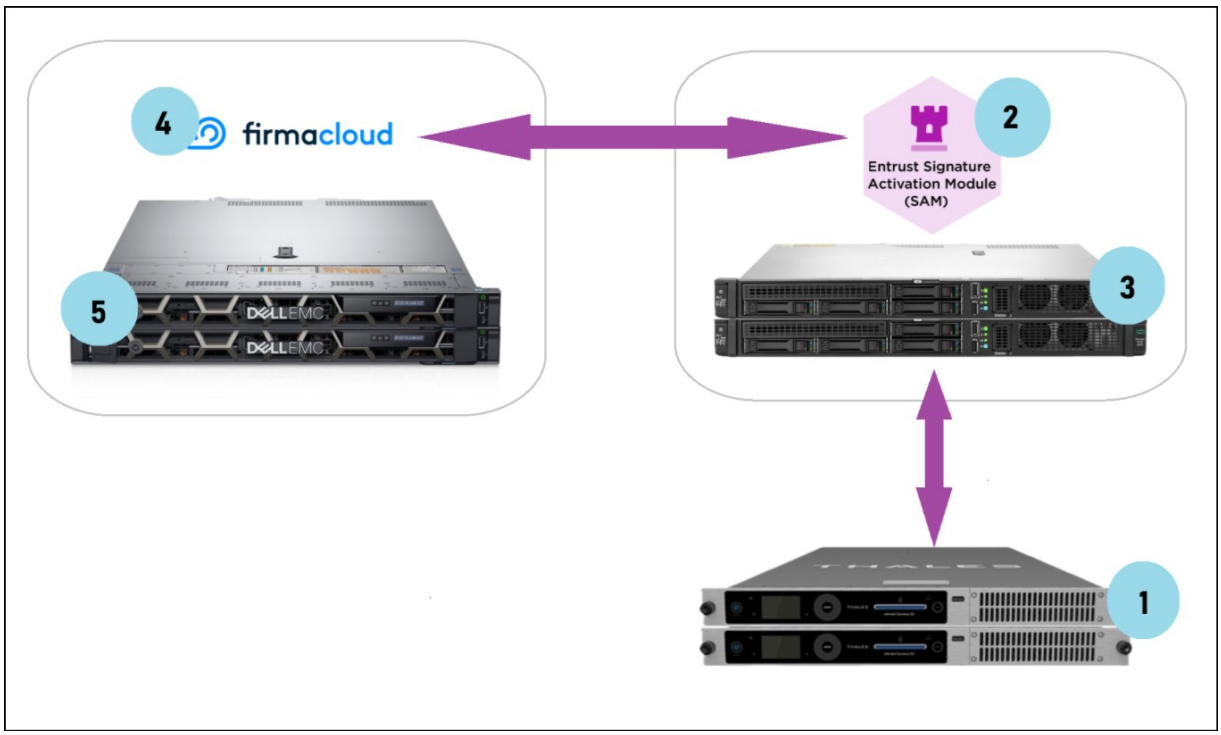
9.6.5 Representations and guarantees of other participants 51
9.7 Disclaimer of warranty 51
9.8 Limitations of liability 51
9.9 Indemnification 51
9.10 Period of validity and termination 52
9.10.1 Term 52
9.10.2 Termination 52
9.10.3 Effect of termination and survival 52
9.11 Notices and individual communications with participants 52
9.12 Modifications or changes in specifications 52
9.12.1 Procedure for changes 52
9.12.2 Notification mechanism and deadline 52
9.12.3 Circumstances in which the OID must be modified 53
9.13 Provisions for conflict resolution 53
9.14 Applicable regulations 53
9.15 Compliance with applicable regulations 53
9.16 Miscellaneous provisions 53
9.16.1 Entire Agreement 53
9.16.2 Independence 54
9.16.3 Judicial resolution 54
9.16.4 Enforcement (attorneys' fees and waiver of rights) 54
9.16.5 Force majeure 54
9.17 Other provisions 54

1. Introduction

1.1. Summary

The Firmaprofesional remote qualified electronic signature generation system is made up of the following elements:

1. HSMs nCipher Connect XC
2. Software SAM Entrust.
3. Server HPE tamper proof Proliant DL20, Intel Xeon E-2436 2.9G, 2x 16GB RAM RDIMM, 2x 240GB SSD SATA.
4. Viafirma Fortress software hardened in collaboration with Firmaprofesional
5. Server DELL EMC *tamper proof* modelo Power Edge R440, Intel Xeon Silver 4210R 2.4G, 2x 16GB RAM RDIMM, 2x 480GB SSD SATA



1.2. Identification of the Document

Name:	Statement of Practices and Remote Qualified Electronic Signature Service Policy (SPPS) of Firmaprofesional, S.A.
Version:	240801
Description:	Statement of Practices and Remote Qualified Electronic Signature Service Policy (SPPS) of Firmaprofesional, S.A.
Date of Issuance:	01/08/2024
OIDs:	1.3.6.1.4.1.13177.30.8.1
Location:	http://www.firmaprofesional.com/cps

1.3 Participating Entities

1.3.1. Certification Authorities (CA)

All certificates described in this Policy must be issued by Firmaprofesional as a Trust Services Provider that issues qualified certificates according to Law 6/2020, and in accordance with Regulation EU 910/2014 (eIDAS).

Corporate certificates, personal certificates and Civil Servant certificates are issued by the Subordinate Certification Authority (CA) "AC Firmaprofesional - CUALIFICADOS".

1.3.2 Registration Authorities (RA)

The management of the applications and the issuance of the certificates will be carried out by the entities that act as Firmaprofesional Registration Authorities..

Each Registration Authority shall establish:

- The criteria to be complied with in order to request a certificate, without contradiction with the CPS and this CP.
- The necessary mechanisms and procedures to perform both identification and authentication of the signatory, in compliance with the CPS and this CP.

- Signature Creation Devices to be used, from those approved by Firmaprofesional.

Corporation or Professional Association acting as RA may delegate these functions to a trust entity when the geographical location of the subscribers (see section 2.4) presents a logistical problem for the applicant identification and/or subsequent delivery of the certificate. In order to justify this delegation, the trust entity shall have a specific connection with the RA and a close relationship with the applicants.

The trust entity shall sign a collaboration agreement with the RA accepting the delegation of these functions. Firmaprofesional must expressly and previously authorize the template or model of agreement to be signed.

1.3.3 Subscribers

The Subscriber is the natural or legal person who has contracted the trusted services of Firmaprofesional and who, therefore, will be the owner of the certificate, and who will have the rights of revocation and suspension on the certificate.

Depending on the type of Certificate, the Subscriber may be:

- The Professional Association in the Corporate Certificates for Professional Association Members.
- The Corporation in the Corporate Certificates of Natural Person and in all those of Representatives (of entities with or without Legal Status).
- The applicant himself, in the case of personal certificates
- The Public Administration, Body or Entity under public law, in the Civil Servant and Civil Servant with a pseudonym Certificates.

1.3.3.1. Applicant

Natural person of legal age who, in their own name, requests the issuance of a certificate to Firmaprofesional.

For specific Certificates, the natural person will need to be endowed with a special condition. Therefore, they may request certificates depending on each type:

- Corporate Certificates for Professional Association Member:

- Any member of the professional association.
- The Professional Association itself, on behalf of the members.

- Corporate Certificates for Natural Person:
  - The legal or voluntary representative of the Corporation, or person/s authorized by such, on behalf of the employees or the person/s associated to such Corporation.
  - Any person/s associated with a Corporation acting as an RA of Firmaprofesional, according to the criteria established by such Corporation.
  - Self-employed professionals or sole proprietors. Since they have no legal personality, they may request a Corporate Certificate for Natural Person where the identities of both natural and legal persons are the same.
- Corporate Certificates for Representative without Legal Personality:
  - Representative of the Entity without Legal Personality with general powers to act towards the Public Administration, being the subscriber of the certificate.
- Corporate Certificates for Legal Representative:
  - The administrator or the representative with general powers.
- Corporate Certificates for Voluntary Representative towards Public Administration:
  - Voluntary representative of the Corporation with general powers to act towards Public Administration of the Corporation, being the subscriber.
- Certificates for Civil Servant and Civil Servant with pseudonym:
  - Civil Servant that depends on a Public Corporation established as an RA of Firmaprofesional.

1.3.3.2. Signatory

The signatory is the natural person that creates the electronic signature. For this purpose, they must be identified with their name, surnames and documentation (NIF, NIE or Passport Number), except in the case of Certificates for Civil Servant with pseudonym, where the natural person shall be identified by a pseudonym.

1.3.4. Third parties trusting in certificates

All certificates described in this Policy are qualified certificates that comply with requirements established in Law 6/2020 and the eIDAS Regulation.

Third parties that trust in these certificates must acknowledge their use limitations, both quantitative and qualitative, contained within the CPS, this CP and the certificate itself.

Finally, all certificates issued under this Policy are recognised by @firma, Validation and Electronic Signature Platform of Spanish Government.

1.3.5 Other participants

No stipulation.

1.4. Certificates use

1.4.1. Appropriate use of certificates

Certificates issued by Firmaprofesional may be used in accordance with terms established by the regulation in force applicable to electronic signature, with additional conditions established in the CPS and this CP.

Furthermore, certificates issued under this CP may be used for the following purposes:

- Guarantee the signatory identity.
- Guarantee the integrity of a signed document.
- Identify the signatory of a document. For Civil Servant Certificates with pseudonym, identification shall be via the pseudonym.

These certificates may be used for relations between the signatory and Public Administration, for strictly defined uses. In cases of Certificates for Voluntary Representative towards Public Administration, the powers attributed to that representative will define usage limits.

1.4.1.1. Certificate Validity Period

The validity period will be as indicated within the certificate itself. This period may be until a maximum of 5 years for all certificates contained within this Policy except Certificates for Civil Servant and Certificates for Civil Servant with pseudonym, where the period may be until a maximum of 4 years.

Certificates with an e-mail protection extension whose root CA is in the browsers will have a maximum validity period of 3 years.

1.4.1.2. Signature Creation Qualified Devices

In cases where Firmaprofesional is able to guarantee that the cryptographic keys of the signatory are created in a Qualified Signature Creation Device (QSCD), whether portable or centralized, in accordance with requirements established within Annex II of Regulation EU 910/2014 eIDAS, this condition will be indicated in the certificate via the following fields:

- Extension "Certificate Policies" with OID value set to the Firmaprofesional certification policy relating to High-Level Certificate with portable or centralized QSCD.
- Extension QcStatement with value "id-etsi-qcs-QcSSCD" enabled .

1.4.2. Non authorized use of certificates

Usage that contravenes Spanish and European Community regulations, international conventions ratified by the Spanish state, customs, moral and public order is not allowed. Neither is any use not defined within this CP or the CPS permitted.

In addition, use of certificates for Civil Servant (with or without pseudonym) for any use other than as defined by Law 40/2015, 1st October, for Public Sector Legal Regime is not allowed.

Use of certificates issued under this CP is not recommended for document encryption.

1.5 Policy Administration

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

1.5.1 Organization managing the document

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

1.5.2 Contact person

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

1.5.3 Person who determines the suitability of the CP for the policy

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

1.5.4 CP approval procedure

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

1.6 Definitions and acronyms

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

2. Repositories and Publication of Information

2.1 Repositories

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

2.2 Publication of certification information

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

2.3 Time or frequency of publication

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

2.4 Repositories access control

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

3. Identification and Authentication

3.1 Registration of Names

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

3.1.1 Types of names

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

3.1.2 Need for names to be meaningful

The DN fields referring to the Name and Surname will correspond to the legally registered data of the signatory, expressed exactly in the format that appears in the National Identity Document, residence card, passport or other means admitted by law.

3.1.3 Anonymity or pseudonymity of subscribers

Only "public employee certificates with a pseudonym or with a professional identification number" are allowed the use of a pseudonym.

3.1.4 Rules for interpreting various forms of names

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

3.1.5 Uniqueness of names

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

3.1.6 Recognition, Authentication and Role of Trademarks

No stipulation

3.2 Initial validation of identity

3.2.1 Private key possession test method

According to the provisions of the current Certification Practices Statement of Firmaprofesional

3.2.2 Authentication of the organization's identity and domain identity

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

3.2.3 Authentication of the identity of a natural person

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

3.2.4 Unverified subscriber information

Without stipulation.

3.2.5 Validation of the identity of the RA and its operators

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

3.2.6 Interoperability criteria

Currently Firmaprofesional does not have cross certification.

3.3 Identification and authentication for key renewal requests

3.3.1 Identification and authentication for password change

The same steps must be followed as for issuing a new certificate (4.3 Certificate issuance).

3.3.2 Identification and authentication for the renewal of certificates after their revocation

The same steps must be followed as for issuing a new certificate (4.3 Certificate issuance).

3.4 Identification and authentication for revocation request

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

4. Certificate life cycle operational requirements

4.1. Application

4.1.1 Who can submit a certificate request

Applications for these certificates will be made by individuals through Firmaprofesional Registration Authorities.

4.1.2 Certificate application process and responsibilities

Steps to obtain a certificates are as follows:

As a general rule for all certificates contained within this document, applications may be performed directly towards Firmaprofesional or via a collaborator acting as RA of Firmaprofesional.

In cases of Corporate Certificates for Natural Person, Corporate Certificates for Professional Association Member, Certificates for Civil Servant (with pseudonym or with a professional identification number), the Corporation or Public Administration acting as RA of Firmaprofesional may process applications directly and proceed to issue certificates by accessing to the management and issuance systems of Firmaprofesional. For this purpose, users wanting to request a certificate must contact their Organization and perform the application by the established means.

In the case of Personal Certificates, applications may also be performed using a current qualified electronic certificate, providing that Firmaprofesional may automatically prove the last date when the applicant presented itself towards the Trust Services Provider to which that current certificate belongs.

4.2 Processing of certificate applications

4.2.1 Performing identification and authentication functions

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

4.2.2 Approval or denial of certificate applications

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

4.2.3 Processing time for certificate requests

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

4.3 Certificate issuance and Initialization of the signing keys

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

4.3.1 Actions of the CA during the issuance of the certificate

4.3.1.1. Generation of signing keys

'The SSASC uses the server-side signing application 'firmacloud' in combination with the Entrust SAM software installed on a tamper-proof server, together with a Connect XC cryptographic module (HSM) acting as SCDev / QSCD, which is a qualified signature creation device."

The SSASC uses HSMs has been validated to meet at least FIPS 140-2 level 3, FIPS 140-3 level 3, or an appropriate certification and Common Criteria EAL 4+ (or higher) to perform all cryptographic operations with signer keys [SRG_KM.1.1]

'The signers' keys are RSA keys with a key length of 2048 bits and elliptic curve secp256r1 keys with a key length of 256 bits." [SRG_KM.1.2]

Outside the HSM module, the keys are stored encrypted with the AES algorithm and a key length of 128 bits. The encryption key is unique and is derived from a master key of the HSM module. [SRG_KM.1.3]

Cryptographic module management initialization operations require dual control. [SRG_KM.1.4]

The key pairs of the signatories are generated in the first phase of the process of issuing the signer's electronic certificate.

Before importing the signatory certificate, the signatory key pair is in a non-active state and SSASC does not allow its use. [SRC_SKS.1.3]

Along with the signatory's key, the SSASC generates a certificate request in PKCS#10 format that serves as proof of possession of the signer's private key in the process of registering the certificate and issuing the certificate by the Certification Authority.

4.3.1.2. Association of the electronic identification means of the signatory

The operator of the Registration Authority is authenticated by means of a client certificate through a secure channel to the interface of the Registration Authority.

The Registration Authority validates the identity of the signatory in accordance with the requirements established in the Certification Practices Statement of the certificate requested

by the signatory with a high level of guarantee according to the requirements established in EU 2015/1502. [LNK-6.2.2-01] [LNK-6.2.2-02]

Parts of the identification and authentication process of the signatory for the signing act are not delegated to third parties.

The Registration Authority stores the data of the signatory, including their telephone number, and requests the SSASC to create a pair of keys that links the signatory in the database. [LNK-6.2.2-03]

The Registration Authority requests from the Certification Authority the electronic certificate linked to the pair of keys generated in the SSASC.

The Registration Authority requests the SSASC to link the issued certificate to the signatory's key pair. [LNK-6.2.2-05]

The Registration Authority will deliver a single-use registration code to the signatory by email to complete the registration process.

The electronic identification means of the signatory are generated by the signatory by accessing the SSASC with a web browser through a secure protocol.

Once the SSASC verifies that the user has activated two authentication factors of different categories, it enables the use of the signatory's private key.

SSA protects the integrity of signatory's keys and their associated metadata through database association [LNK-6.2.2-10]

4.3.1.3. Signatory certificate association

Once the signatory certificate registration and issuance process has been completed, the signatory certificate is imported into the SSASC.

The SSASC verifies that the public key in the signatory's certificate and the one stored in the system relate to each other [LNK-6.2.3-01].

If both public keys match, the certificate is linked to the signatory's key pair.

The signatory's key is marked as inactive and waits for the signatory to activate their signature activating factors. [LNK-6.2.3-02].

SSASC protects the integrity of signatory's keys and their associated metadata through database association. [LNK-6.2.3-03] [SRC_SKS.1.5]

4.3.1.4. Provision of means of the signatory identification

The means of identification of the signatory are generated by the signatory him or herself, accessing the SSASC with a web browser through a secure protocol.

The seed for the one-time passwords (OTP) is stored encrypted in the SSASC database and protected by an AES key, which is in turn secured by the cryptographic module, and is randomly generated by the SAM

The SSASC in no case stores the passwords of the signatory, only hashes to be able to verify their validity.

4.3.2 Notification to the subscriber by the CA of the issuance of the certificate and delivery

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

4.4 Certificate acceptance

4.4.1 Form in which the certificate is accepted

The certificate will be accepted when the binding legal instrument between the subscriber and Firmaprofesional has been signed and the certificate has been delivered, either personally or electronically.

As evidence of acceptance, there must be an acceptance sheet signed by the signatory. The certificate will be considered valid from the date the acceptance sheet was signed.

If the acceptance sheet is in electronic format, the signatory may sign it by means of an electronic signature.

4.4.2 Certificate publication by the CA

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

4.4.3 Notification of the issuance of the certificate by the CA to other entities

Without stipulation.

4.5 Use of keys and certificate

4.5.1 Use of the subscriber's certificate and private key

The certificates issued under this CP can be used to identify the subscriber and to sign electronic documents and files.

4.5.1.1. Activation of signing keys

For each use of their signature key, the signatory must provide a signature activation message (SAD) through the signature activation protocol (SAP). The message must contain two authentication factors of different types and a witness. **[SIG-6.3.1-01] [SIG-6.3.1-05**]

To obtain a witness, the SSASC requires the signatory to previously identify him or herself with their user and at least one authentication factor.

Signatory keys can only be activated if the HSM module is active. **[SIG-A.5-02]**

A signatory's key is only activatable if the signatory completes the activation protocol (SAP) and the authentication factors sent in the SAD are correct. **[SIG-6.3.1-09]**

The Signature Activation Protocol (SAP) is designed to prevent man-in-the-middle and replay attacks **[SIG-6.3.1-02]**. In addition to this, the SAD message incorporates protections against impersonation, session theft, duplication, credential theft, phishing, listening and guessing, through the combination of encryption techniques, electronic signature, summary functions, incorporation of random data and two authentication factors. of a different nature (something that the signatory knows and something that the signatory owns). If the signatory wrongly enters the activation factor 3 consecutive times, access to the remote key is blocked. A blocked remote key can only be unlocked by the signatory him or herself by entering a recovery sent to their email **[SIG-6.3.1-06] [SIG-A.5-04] [SIG-A.5-06] [SIG-A.5-07]**.

Activation factors are always transported through a secure communication protocol within the key activation message (SAD) [SIG-A.5-03]

The access controls implemented in the SSASC guarantee that a signatory does not have access to the keys of other signatories or to other objects and functions of the system that are not the signature functions or their personal management [SIG-6.3.1-03]

The signature activation message (SAD) links the cryptographic summary of the data to be signed with the signatory's activation data through the session token included in the message. [SIG-6.3.1-04]

Once the signatory's key is activated, the SSASC only allows its use to sign the cryptographic summary contained in the SAD message used for activation [SIG-6.3.1-07]. Once the requested signature operation is carried out with the SAD, the SSASC deactivates the signatory's key, requiring a new SAD for a new signature.

The SSA stores in the signatory's key pair metadata the expiration date of the associated certificate. Before the use of a signing key, the SSASC checks that the expiration date of the certificate is valid and the revocation status of the certificate, and denies the operation according to the status of the certificate. [SIG-6.3.1-08]

All communications with the SSASC are protected using the TLS 1.2 protocol.

"The SSASC allows generating rsa-pkcs1, rsa-sha256, rsa-sha384, rsa-sha512, and ecdsa signatures [SIG-6.3.1-10]."

4.5.1.2. Signature activation data management

The message with the signature activation data (SAD) is generated from a single-use code generated in an application from a previous seed or received via SMS generated by the SSASC itself [SIG-A.6-02]

The SAD message contains the cryptographic summary(s) of the data to be signed, references that allow the selected key to be identified and the signer to be identified, the encrypted signature activation PIN. The entire SAD message is signed with the signature activation private key in the SAA application to authenticate the signer. [SIG-A.6-01] [SIG-A.6-03] [SIG-A.6-06]

The SSASC only allows the signer to use their signature activation key from a single smartphone, thus avoiding duplication. [SIG-A.6-06]

The combination of two different authentication factors and the session token ensure that the signer has exclusive control of their signature activation data. [SIG-A.6-07]

The SAP consists of the transmission of a single SAD message through a secure channel to the SSA. The signature activation module (SAM) is a sub-module of the SSA [SIG-A.6-05]

The AVA_VAN.5 level of evaluation of the SSA solution has considered high potential attackers in the security tests in order to ensure that the authentication mechanism to activate the signature creation data cannot be altered. [SIG-A.6-08]

4.5.1.3. Signing keys deletion

The signatory keys are deleted immediately, when the signatory's certificate is revoked.

Firmaprofesional periodically executes a process of deleting those keys of the signatories whose associated certificate has expired. **[DEL-6.3.2-01]**

The signatories may request the revocation of their electronic certificate following the mechanisms established in the corresponding Certification Practices Statement. The revocation and expiration of the certificate implies in all cases the destruction of the associated keys. **[DEL-6.3.2-02]**

4.5.1.4. Backup and restore of signing keys

The signatory keys are protected by the master key of the cryptographic module; they can only be used when the cryptographic module is active.

When backing up signatory keys, the AES encryption algorithm and a key length of 128 bits are used. [GEN-6.3.3-01] [GEN-6.3.3-02]

Periodic backup copies of the SSA database are kept, where the passwords of the signatories are referenced, and the rest of the infrastructure passwords necessary to guarantee the continuity of the service in the event of an incident.

SSASC infrastructure keys are always stored in encrypted containers.

The cryptographic module that contains the master key of the SSASC that protects the keys of all the signatories requires dual control for its operation, backup and restoration. The SSASC master key never leaves the cryptographic module in the clear. [GEN-6.3.3-03]

The number of backup copies is the minimum to guarantee the continuity of the service. [GEN-6.3.3-04]

4.5.2 Use of Trusting Party Certificates and Public Keys

Third parties who trust the certificates may use the certificates for what is established in this CP and the CPS.

It is the responsibility of the third parties to verify the status of the certificate through the services offered by Firmaprofesional specifically for this, and specified in the CPS.

4.6 Renewal of the certificate (without change of keys)

No stipulation except when there is a change of keys that will be governed by the provisions of point 4.7.

4.6.1 Circumstance for certificate renewal

Without stipulation.

4.6.2 Who can request renewal

Without stipulation.

4.6.3 Processing certificate renewal requests

Without stipulation.

4.6.4 Notification to the subscriber of the issuance of a new certificate

Without stipulation.

4.6.5 Conduct that constitutes acceptance of a renewal certificate

Without stipulation.

4.6.6 Publication of the renewal certificate by the CA

Without stipulation.

4.6.7 Notification of the issuance of the certificate by the CA to other entities

Without stipulation.

4.7 Certificate renewal with password change

4.7.1 Circumstance for changing the certificate key

The certificate can only be renewed if the following conditions are met:

- The certificate has not expired.
- In the case of qualified certificates, less than 5 years have elapsed since their last appearance and identification with the RA in accordance with current regulations.

4.7.2 Who can request the certification of a new public key

Any signatory may request the renewal of their certificate if the circumstances described in the previous point are met.

4.7.3 Processing certificate key change requests

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

4.7.4 Notification to the subscriber of the issuance of a new certificate

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

4.7.5 Conduct that constitutes acceptance of a certificate with a new key

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

4.7.6 Publication of the certificate with a new key by the CA

According to the provisions of the current Certification Practices Statement of Firmaprofesional

4.8 Modification of the certificate

In case of need to modify any data, the RA must proceed to revoke and issue a new certificate.

4.8.1 Circumstance for the modification of the certificate

Without stipulation.

4.8.2 Who can request the modification of the certificate

Without stipulation.

4.8.3 Processing certificate modification requests

Without stipulation.

4.8.4 Notification to the subscriber of the issuance of a new certificate

Without stipulation.

4.8.5 Conduct that constitutes acceptance of the modified certificate

Without stipulation.

4.8.6 Publication of the certificate modified by the CA

Without stipulation.

4.8.7 Notification of the issuance of the certificate by the CA to other entities

Without stipulation.

4.9 Revocation and suspension of certificates

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

4.9.1 Circumstances for revocation

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

4.9.2 Who can request revocation

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

4.9.3 Revocation request procedure

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

4.9.4 Grace period for revocation request

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

4.9.5 Time within which CA must process the revocation request

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

4.9.6 Revocation verification requirement for relying parties

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

4.9.7 CRL emission frequency

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

4.9.8 Maximum latency for CRLs

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

4.9.9 Online Revocation / Status Check Availability

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

4.9.10 Online revocation verification requirements

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

4.9.11 Other forms of revocation announcements available

Without stipulation.

4.9.12 Special requirements related to the key engagement

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

4.9.13 Circumstances for suspension

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

4.9.14 Who can request suspension

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

4.9.15 Suspension request procedure

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

4.9.16 Limits of the suspension period

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

4.10 Certificate status services

4.10.1 Operational characteristics

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

4.10.2 Service availability

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

4.10.3 Optional functions

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

4.11 Termination of subscription

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

4.12 Custody and recovery of keys

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

4.12.1 Key custody and recovery policy and practices

Without stipulation.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Without stipulation.

5. Physical security, facilities, management and operational controls

5.1 Physical controls

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

5.1.1 Site location and construction

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

5.1.2 Physical access

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

5.1.3 Energy and air conditioning

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

5.1.4 Exposure to water

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

5.1.5 Fire prevention and protection

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

5.1.6 Media storage

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

5.1.7 Waste disposal

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

5.1.8 Off-site backup

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

5.2 Procedural controls

5.2.1 Trusted roles

The SSA implements the following management roles:

- Security Officer: Has overall responsibility for managing and implementing security policies and has access to security information.
- System administrator: is responsible for installing, configuring and maintaining the TW4S but with controlled access to security information.
- System operator: is responsible for the day-to-day operation of TW4S and backup and restore operations.
- System auditor: is authorized to review the files and audit logs of the TW4S to audit that the system operations are aligned with the security policy.

Firmaprofesional assigns these roles to qualified personnel and implements all the segregation of duties controls defined in section 6.2.1.2 of the CEN EN 419 241-1 standard.

[OVR-6.5.1-01]

5.2.2 Number of people needed per task

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

5.2.3 Identification and authentication for each role

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

5.2.4 Roles requiring separation of duties

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

5.3 Personnel controls

5.3.1 Qualifications, experience and authorization requirements

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

5.3.2 Background check procedures

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

5.3.3 Training requirements

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

5.3.4 Frequency and requirements of retraining

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

5.3.5 Frequency and sequence of job rotation

Without stipulation.

5.3.6 Sanctions for unauthorized actions

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

5.3.7 Requirements for independent contractors

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

5.3.8 Documentation provided to personnel

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

5.4 Audit log procedures

See the corresponding section in the Firmaprofesional Certification Practices Statement **[OVR-6.4.5-01] [OVR-6.4.5-02]**

The SSASC keeps a record of at least the following events:

- System initialization, startup, shutdown and configuration changes.
- Signatory key management events (generation, activation, use, deactivation, and destruction)
- Use of signatory keys.
- Authentication of the signatory (including failed attempts).

- Management of signatory signature activation data (PIN changes)
- Start and stop of the audit functions.
- Changing the configuration of the audit functions.
- System access by administrator users.

The SSAC automatically stops processing requests if its audit functions are unavailable. [OVR-6.4.5-03]

The SSAC generates a continuous audit trail where only new events can be added and old events cannot be deleted or modified.

SSAC protects audit log events at the entry level and throughout the log by applying a unique logging index. [OVR-6.4.5-04]

All SSA audit log event logs include the following information:

- Date and time of the event.
- Event type.
- Identity of the entity (signatory, administrator or process) responsible for the action.
- Event result (success or failure) [OVR-6.4.5-05]

The SSASC checks the integrity of the audit trail at startup and periodically to detect deletion or modification. Additionally, the SSA has a functionality to verify the integrity of the audit record at the request of a user with an auditor role in the system. [OVR-6.4.5-06]

To guarantee the accuracy of the date and time of the audit events, the system clock is synchronized by NTP using the ROA (Royal Observatory of the Navy) as a reference. Checks are in place to detect problems that could compromise synchronization. [OVR-6.4.5-07]

5.5 Log file

According to the provisions of the current Certification Practices Statement of Firmaprofesional. **[OVR-6.4.6-01]**

5.6 Password change

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

5.7 Disaster recovery plan

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

5.8 Cessation of activity of the RA or CA

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

6. Technical security controls

6.1 Key pair generation and installation

"The entity has procedures in place to correctly and securely operate the SSASC. [OVR-6.5.2-01]

The SSA software component, the Entrust SAM, and the HSM module are operated in accordance with their installation, administration, and operation manuals to meet the security objectives defined in the Security Statement of their Common Criteria certification. [OVR-6.5.2-02] [GEN-A.4-02] [GEN-A.5-02]"

6.2 Private key protection and cryptographic module engineering controls

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

6.3 Other aspects of key pair management

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

6.4 Activation data

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

6.5 IT security controls

According to the provisions of the current Certification Practices Statement of Firmaprofesional. **[OVR-6.5.3-01]**

The SSASC is monitored and alerts are generated that are sent to the system administrators when events are detected that may impact its availability or compromise its security [OVR-6.5.3-02]

Additionally, the monitoring system allows generating alerts based on correlation rules to detect behaviors that may indicate a potential attack.

6.6 Technical life cycle controls

According to the provisions of the current Certification Practices Statement of Firmaprofesional. [**OVR-6.5.4-01]**

6.7 Network security controls

According to the provisions of the current Certification Practices Statement of Firmaprofesional. **[OVR-6.5.5-01]**

6.8 Time control

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

7. Profiles of certificates, CRL and OCSP

7.1 Certificate profile

7.1.1 Version number

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

7.1.2 Certificate extensions

The extensions used by each type of certificate issued under this policy are published in the document called "Profiles of Firmaprofesional certificates" on the Firmaprofesional website (http://www.firmaprofesional.com/cps).

7.1.3 Algorithm object identifiers

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

7.1.4 Name forms

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

7.1.5 Name restrictions

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

7.1.6 Certificate policy object identifier

In accordance with the prescriptions contained in this document, the following types of certificates are issued, with their associated OIDs:

Type of Certificate	**OID**
Corporate Certificates for Professional Association Member. High-Level with centralised QSCD	1.3.6.1.4.1.13177.10.1.1.3
Corporate certificates for Natural Person. High-Level with centralised QSCD	1.3.6.1.4.1.13177.10.1.2.3
Corporate Certificates for Legal Representative. Within centralised QSCD	1.3.6.1.4.1.13177.10.1.11.3
Corporate Certificates for Voluntary Representative towards Public Administration. Within centralised QSCD	1.3.6.1.4.1.13177.10.1.12.3
Corporate Certificates for Representative of Entity without Legal Personality. Within centralised QSCD	1.3.6.1.4.1.13177.10.1.13.3
Certificates for Civil Servant. High-Level with centralised QSCD	1.3.6.1.4.1.13177.10.1.22.3

Personal Certificates. Within centralised QSCD	1.3.6.1.4.1.13177.10.1.40.3

7.1.7 Using the Policy Constraints extension

Without stipulation.

7.1.8 Syntax and semantics of policy qualifiers

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

7.1.9 Processing semantics of the critical Certificate Policies extension

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

7.2 CRL profile

7.2.1 Version number

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

7.2.2 CRL extensions and CRL entries

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

7.3 OCSP profile

7.3.1 Version number

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

7.3.2 OCSP extensions

Without stipulation.

8. Compliance audits and other controls

8.1 Frequency of audits

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

8.2 Qualification of the auditor or evaluator

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

8.3 Relationship between the auditor and the audited authority

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

8.4 Aspects covered by the evaluation

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

8.5 Actions to be taken as a result of the detection of deficiencies

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

9. Other legal and business issues

9.1. Rates

Firmaprofesional will charge the Subscriber as agreed within the service delivery contract signed by both parties.

Firmaprofesional may establish rates it considers appropriate to subscribers, as well as the payment methods it considers suitable for each case. For further details about rates and payment conditions, the Sales Department of Firmaprofesional should be consulted.

9.1.1 Certificate issuance or renewal fees

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

9.1.2 Certificates access fees

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

9.1.3 Revocation or status information access fees

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

9.1.4 Fees for other services

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

9.1.5 Reimbursement fees

Without stipulation.

9.2 Financial responsibilities

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

9.2.1 Insurance coverage

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

9.2.2 Other assets

Without stipulation.

9.2.3 Insurance or guarantee coverage for end entities

Without stipulation.

9.3 Confidentiality of commercial information

9.3.1 Scope of confidential information

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

9.3.2 Non-confidential information

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

9.3.3 Responsibility to protect confidential information

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

9.4 Protection of personal information

9.4.1 Personal data protection policy

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

9.4.2 Information treated as private

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

9.4.3 Information not considered private

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

9.4.4 Responsibility to protect private information

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

9.4.5 Notice and consent to the use of private information

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

9.4.6 Disclosure under judicial or administrative process

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

9.4.7 Other information disclosure circumstances

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

9.5 Intellectual property rights

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

9.6 Obligations and guarantees

9.6.1 Obligations of the CA

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

9.6.2 Obligations of the RA

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

9.6.3 Obligations of applicants

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

9.6.4 Representations and guarantees of third parties who trust the certificates

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

9.6.5 Representations and guarantees of other participants

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

9.7 Disclaimer of warranty

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

9.8 Limitations of liability

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

9.9 Indemnification

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

9.10 Period of validity and termination

9.10.1 Term

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

9.10.2 Termination

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

9.10.3 Effect of termination and survival

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

9.11 Notices and individual communications with participants

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

9.12 Modifications or changes in specifications

9.12.1 Procedure for changes

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

9.12.2 Notification mechanism and deadline

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

9.12.3 Circumstances in which the OID must be modified

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

9.13 Provisions for conflict resolution

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

9.14 Applicable regulations

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

9.15 Compliance with applicable regulations

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

9.16 Miscellaneous provisions

9.16.1 Entire Agreement

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

9.16.2 Independence

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

9.16.3 Judicial resolution

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Without stipulation.

9.16.5 Force majeure

According to the provisions of the current Certification Practices Statement of Firmaprofesional.

9.17 Other provisions

Without stipulation.