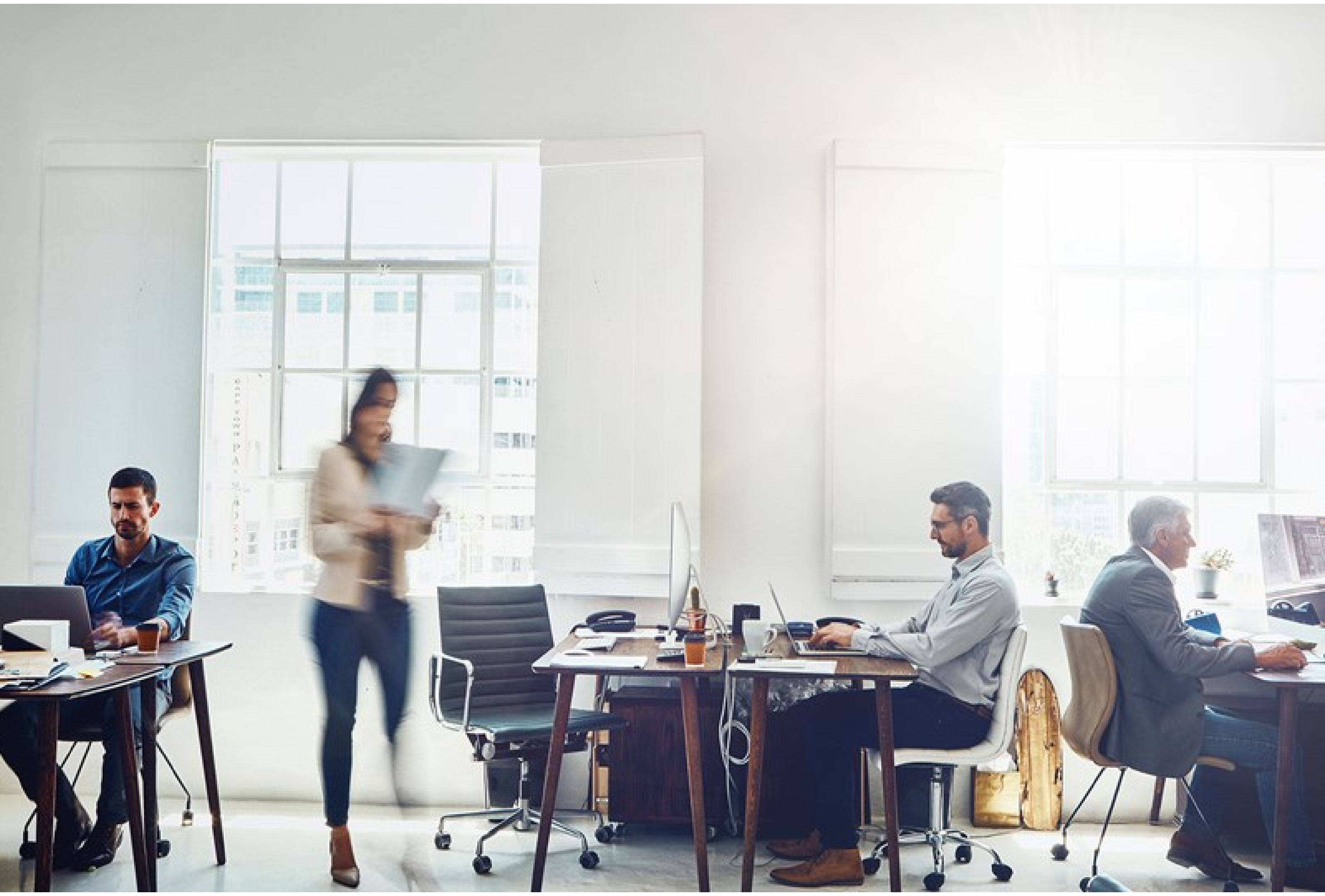
Certification Policy

Electronic signatures certificates

Version: 240123

Classification: Public

Firmado digitalmente por: FIRMAPROFESIONAL, S.A.Fecha y hora: 11.03.2024 18:34:25



Version history

Version	Section and changes	Date of publication
190121	• New Certification Policy for Personal Certificates that groups together all existing policies regarding this type of certificate. May be consulted at http://firmaprofesional.com/cps	21/01/2019
190507	• Added verification of the applicant's email before the issuance of the certificate. • Restructured the OIDs, eliminating duplicities. • Error correction. • Changed the CA that issues the Public Servant certificates to "AC Firmaprofesional - CUALIFICADOS".	07/05/2019
200417	• Added measures due to COVID-19 Spanish Alarm Status. • Added the possibility of issuing the "Personal Certificates. Within centralised QSCD / 1.3.6.1.4.1.13177.10.1.40.3 "	17/04/2020
210217	• Adaptation to the new Law 6/2020, regulating certain aspects of electronic trust services	17/02/2021
220216	• Adaptation to RFC3647 • Added reference Pseudonym certificates as certificates with professional identification number in accordance with RD 203/2021	16/02/2022
220510	• Added OID 1.3.6.1.4.1.13177.10.1.14 • Update section 1.4.1.1	10/05/2022
230616	• Update section 1.4.1.1: limitation up to 3 years certificates issued in QSCD card or token • Update section 1.3.1 • Update section 3.1	16/06/2023
230828	• Modification of section 1.4.1 Appropriate uses of certificates: clarifications on the use of electronic signature certificates with Public Administrations	28/08/2023
240123	• Modification of section 1.4.1.1 to extend the validity of public employee certificates from 4 to up to 5 years.	23/01/2024

Index

1. Introduction

1.1. Summary

Electronic signature certificates, as defined within Regulation EU 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions (hereafter "eIDAS"), are electronic statements that associate validation data of a signature with a natural person, and confirm name or pseudonym of that person.

All certificates contained in this Policy are Recognised Certificates for Natural Person for Electronic Signature according to Law 6/2020, of November 11, regulating certain aspects of electronic trust services (hereinafter, Law 6/2020 LSEC), and meet the requirements established in Annex I of the eIDAS Regulation.

Request and issuance of these certificates may be performed via Firmaprofesional Registration Authorities enabled for this purpose.

The Registration Authority may be different depending on each Certificate. This Certification Policy (hereafter "Policy" or "CP") contains three types of Certificates, and their associated Register Authorities are the following:

1. **Corporate**. Three variations:

    a. for Professional Association Members -> Application and issuance are performed via the Professional Associations to which each certificate is linked, and the Professional Association Member obtains it.

    b. for natural Person -> Application and issuance are performed via the Corporations to which each certificate is linked, or via other Registration Authority of Firmaprofesional not associated with the signatory

    c. for Legal Person -> Application and issuance of this type of certificate are performed via the Registration Authorities of Firmaprofesional

        i. Representative of an entity without legal personality

        ii. Legal Representative

        iii. Voluntary Representative

2. **Personal** -> Application and issuance are performed via Registration Authorities of Firmaprofesional enabled for this purpose.

3. **Public Servant** -> Public Servant Certificates are issued in conformity with requirements established within article 43 of Law 40/2015, 1st October, of Public Sector Legal Regime for electronic signature for staff within the service of Public Administrations. These certificates adapt to definitions of high and medium security levels and to certificate profiles established within section 10 of the document "Electronic Certificates Profiles" of Sub-Directorate General of Information, Documentation and Publications of Ministerio de Hacienda y Administraciones Públicas.

   There are two types of certificates:

   a. Certificates for public servant.

   b. Certificates for public servant with pseudonym.

   For both types, application and issuance are performed via the Public Administration, which issues these certificates for public servants, statutory and authorised staff, in the execution of their duties, allowing to telematically identify subscribers as the Public Administrations and signatories as persons within the service of the Public Administration.

Particular conditions referring to all certificates contained in this CP are described in this document. The CP is subject to compliance with the Certification Practices Statement of Firmaprofesional (hereafter "CPS").

1.2. Identification of the Document

Name:	CP Electronic Signature Certificates
Version:	230616
Description:	Certification Policy for Electronic Signature Certificates where all certificates issued to natural persons (with and without attributes) are grouped together.
Date of Issuance:	16/06/2023
OIDs:	1.3.6.1.4.1.13177.10.1.1.D (*) Certificates for Professional Association Member 1.3.6.1.4.1.13177.10.1.2.D (*) Corporate Certificates for Natural Person 1.3.6.1.4.1.13177.10.1.14. D (*) Corporate Certificates for Natural Person to sign emails 1.3.6.1.4.1.13177.10.1.11.D (*) Corporate Certificates for Legal Representative 1.3.6.1.4.1.13177.10.1.12.D (*) Corporate Certificates for Voluntary Representative towards Public Administration 1.3.6.1.4.1.13177.10.1.13.D (*) Corporate Certificates for Representative of Entity without Legal Personality 1.3.6.1.4.1.13177.10.1.22.D (*) Certificate for Public Servant 1.3.6.1.4.1.13177.10.1.23.D (*) Certificate for Public Servant with pseudonym 1.3.6.1.4.1.13177.10.1.40.D (*) Personal Certificates
Location:	http://www.firmaprofesional.com/cps

(*)D = Device / Security Level:

1 = Portable QSCD (High-Level)

2 = Other devices (Medium-level)

3 = Centralised QSCD

This Certification Policy groups together the following Policies, which are repealed with the publication of the version 190121 of this policy:

- Policy of Corporate Certificates for Professional Association Member Version 171121.

- Policy of Corporate Certificates for natural Person Version 171121.
- Policy of Corporate Certificates for Representative of Entity without Legal Personality Version 180328.
- Policy of Corporate Certificates for Legal Representative Version 171121.
- Policy of Corporate Certificates for Voluntary Representative towards Public Administrations Version 171121.
- Policy of Personal Certificates Version 171121.
- Policy of Certificates for Public Servant Version 171121.

All these repealed policies may be consulted on https://www.firmaprofesional.com/cps, section “en el apartado “Previous Policies and Certification Practices”.

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 public servant certificates are issued by the Subordinate Certification Authority (CA) “AC Firmaprofesional - CUALIFICADOS” or “FIRMAPROFESIONAL ICA B01 QUALIFIED 2022”.

1.3.2 Registration Authorities (RA)

Applications management and certificate issuances are performed by the entities acting as Registration Authorities of Firmaprofesional.

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 delegations, the trust entity shall have a specific connection with the RA and a proximity relationship with the applicants.

The trust entity shall sign a collaboration agreement with the RA accepting the delegation of these functions. Firmaprofesional must grant prior and express authorisation for this model agreement.

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 Public Officer and Public Officer with a pseudonym Certificates .

1.3.3.1. Applicant

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

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 member.
- Corporate Certificates for Natural Person:
    - The legal or voluntary representative of the Corporation, or person/s authorised by such, on behalf of the employees or the person/s associated to such Corporation.
    - Any person/s associated to 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 person 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 Public Servant and Public Servant with pseudonym:
  - Public 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 Public Servant with pseudonym, where the natural personal 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 Public 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.

In order to use the certificates with the public Administration, it is necessary that the number of the Spanish National Identity Document, Spanish Foreigner Identification Number or Spanish Tax Identification Number be recorded as part of the holder's identity within the certificate. In any other case, THEY MAY NOT BE USED for the processing with the Spanish Public Administration.

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.

Certificates with an e-mail protection extension whose root CA is in the browsers will have a maximum validity period of 3 years.
Certificates issued in QSCD card or Token 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 centralised, 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 centralised QSCD.
- Extension QcStatement with value "id-etsi-qcs-QcSSCD" enabled .

In all other cases, it will be indicated in the certificate via the following fields:

- Extension "Certificate Policies" with OID value set to the Firmaprofesional certification policy relating to Medium-Level Certificate.
- Extension QcStatement with value "id-etsi-qcs-QcSSCD" disabled .

1.4.2. Non authorised 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 public 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 Firmaprofesional Certification Practices Statement (http://www.firmaprofesional.com/cps).

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.

The limits of the givenName, surname, pseudonym, commonName, and organizationName fields can be greater than the limit established in RFC 5280, according to ETSI 319 412-2 and ETSI 319 412-3.

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 CP, 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 Public 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

It is the RA's responsibility to identify and authenticate the signatory. This process must be carried out prior to the issuance of the certificate.

4.2.2 Approval or denial of certificate applications

A Firmaprofesional RA (Public Body, Professional Association or Corporation), must prove the veracity of the information provided by the applicant.

Depending on the type of certificate, this verification shall be performed using one of the following methods:

a. Corporate Certificates for Professional Association Member: applicant must be a member.

b. Corporate Certificates for Natural Person: Corporation acting as RA may establish the necessary requirements that users must comply with. The RA only may process applications from signatories associated with the Corporation.

   Applications for these certificates performed directly towards Firmaprofesional must add a document signed (by hand or digitally) by the Legal Representative of the Corporation, that authorises the issuance and indicates Name, Surname, DNI and Position within the Organisation. The applicant may request certificates exclusively for those persons previously identified within the last 5 years via their internal procedures. In such cases the signatory does not need to present themselves physically towards Firmaprofesional.

   In cases where the signatory is a sole proprietor, it will only be required that the applicant provides formal documentation proving registration with the Social Security System, as a bank proof with the corresponding payment.

c. Corporate Certificates for Representative without Legal Personality, the verification shall be performed using one of the following methods:

   - Online consultation with Trade Registry.
   - Revision of the notarial documentation provided.
   - Revision of the official bulletin indicated by the applicant.
   - In case where those methods are not followed, it will be necessary to review the provided documentation accrediting the representation of entity without legal personality.

d. Corporate Certificates for Legal or Voluntary Representative. Verification will be performed via online consultation with the Trade Register, reviewing the notarial documentation provided or the official bulletin indicated by the applicant.

e. Personal Certificates. Verification may not be demanded in the following cases:

  - where the identity or other permanent attributes of the applicants are known by the RA due to a pre-existing relationship, by which the means specified in this section were used for the identification of the applicant, and the period of time elapsed since identification is less than five years.

  - When, in order to request a certificate another current certificate is used, where for the issuance of that certificate the signatory has been identified in the manner described in the previous section, and the RA is aware that the period of time elapsed since identification is less than five years.

f. Certificates for Public Servant: the Organisation will validate the identity of the applicant and their role within the Public Administration.

4.2.3 Processing time for certificate requests

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

4.3 Certificate issuance

Each Registration Authority of Firmaprofesional will have a number of accredited persons acting as RA Operators towards Firmaprofesional (regardless the RA is a Professional Association or a Public Body). These RA Operators are authorised by the RA to perform this function and they shall receive a training about certificates issuance. Each RA Operator will have their own Digital Certificate with secure cryptographic device that will allow them to manage users' applications.

4.3.1 Actions of the CA during the issuance of the certificate

In case of Personal Certificates, once the application is approved, and prior to the issuance of the certificate, Firmaprofesional will take reasonable measures to verify the validity of the email provided by the applicant, such as through the exchange of mail with the request for documentation required for the issuance of said certificate or sending random data, which the applicant must access to prove the existence of that email account.

Once the mail has been checked, the necessary information shall be sent to the applicant for them to generate the key pair within their systems. Firmaprofesional receives the certificate application automatically after the keys generation, issues the certificate and provides the means for the applicant to install it in their systems.

However, for the rest of Certificates contained in this Policy, it is necessary to differentiate three phases:

a) **Keys generation**

.

The RA Operator will manage the keys generation for the signatory within a signature creation device, if necessary.

The RA Operator will validate that the signatory has the private key (signature creation data) associated with the public key (signature verification data) included in the certification request.

b) **Certificate issuance**

The RA Operator will generate the certificate request in a standard format and will send it to Firmaprofesional.

Firmaprofesional will validate the integrity of the request and that it is been generated by a RA Operator duly authorised. After this validation, the certificate will be issued.

In cases where Firmaprofesional has certainty that the device in which the key pair has been generated is a QSCD, the certificate will be issued with the corresponding OID.

c) **Delivery**

Once the certificate has been generated, and prior the RA delivers it to the signatory, the signatory must:

- Present themselves in person towards the RA in accordance with article 7 of Law 6/2020 LSEC, except in cases where it is not necessary as described in the article.

- Formally accept the delivery of the certificate leaving documental evidence in the possession of the RA.

Finally, the RA will deliver the certificate to the signatory, either via delivering the portable QSCD, the remote authentication and operational methods, or enabling the mechanisms to download and use it.

For Corporate Certificates for Natural Person, and in cases where the applicant acts on behalf of another natural person, signatory acceptance must be obtained before the certificate is valid. In this case, the certificate will be issued with a grace period during which the certificate will not be valid. Once this period is over, if the applicant has the means to access the private key and has not received the signatory formal acceptance, the applicant will immediately revoke the certificate. Otherwise, the applicant will be considered responsible for any damage resulting from the use of the certificate, specifically regarding to data protection.

Through these procedures, Firmaprofesional guarantees that no signatory has the certificate before their required presentation in-person process has been completed according to article 7 of Law 6/2020 LSEC.

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

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

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.

4.5.2 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.

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

Certificate renewal can be done through the following procedures:

1. In person: the signatory must go personally to the RA of Firmaprofesional and request a new certificate.
2. Online: if the RA has the service, the signer must connect to the online service offered by Firmaprofesional with their current certificate still in force and electronically sign the renewal request or have some other mechanism that allows authenticating their identity and willingness to renew the certificate. The possibility of renewing online will be conditioned by the requirements established by current legislation on electronic signatures. The validity period of certificates renewed online will be conditioned by the requirements established in article 7 of Law 6/2020 LSEC.
3. Automatic (only for Personal Certificates): if the signer accepts this possibility at the time the certificate is issued, before the valid certificate expires, a new certificate with the same keys will be automatically generated. The possibility of automatic renewal will be conditioned by what is established by current legislation on electronic signature.

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

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

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

5.4.1 Types of recorded events

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

5.4.2 Frequency of processing audit records

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

5.4.3 Retention period for audit records

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

5.4.4 Protection of audit logs

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

5.4.5 Back-up procedures for audit records

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

5.4.6 Audit collection system

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

5.4.7 Notification to the subject causing the event

Without stipulation.

5.4.8 Vulnerability analysis

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

5.5 Log file

5.5.1 Types of Archived Records

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

5.5.2 File retention period

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

5.5.3 File protection

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

5.5.4 File backup procedures

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

5.5.5 Requirements for time stamping of records

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

5.5.6 File collection system

Without stipulation.

5.5.7 Procedures for obtaining and verifying file information

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

5.6 Password change

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

5.7 Disaster recovery plan

5.7.1 Incident and engagement management procedures

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

5.7.2 Computer resources, software and / or data become corrupted

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

5.7.3 Procedures for compromising the entity's private key

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

5.7.4 Business continuity capabilities after a disaster

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

6.1.1 Key pair generation

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

6.1.2 Delivery of the private key to the subscriber

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

6.1.3 Delivery of the public key to the certificate issuer

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

6.1.4 Delivery of the CA's public key to relying parties

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

6.1.5 Key size

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

6.1.6 Generation of public key parameters and quality control

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

6.1.7 Key usage purposes (depending on the field of use of the X.509 v3 key)

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

6.2 Private key protection and cryptographic module engineering controls

6.2.1 Cryptographic module rules and controls

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

6.2.2 Multi-person control (k of n) of the private key

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

6.2.3 Private key deposit

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

6.2.4 Private key backup

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

6.2.5 Private key file

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

6.2.6 Transfer of private keys to or from a cryptographic module

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

6.2.7 Storage of the private key in the cryptographic module

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

6.2.8 Private key activation method

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

6.2.9 Private key deactivation method

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

6.2.10 Private key destruction method

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

6.2.11 Cryptographic module classification

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.

6.3.1 Public key file

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

6.3.2 Certificate operation periods and key pair usage periods

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.

6.4.1 Generation and installation of activation data

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

6.4.2 Protection of activation data

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

6.4.3 Other aspects of 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.

6.5.1 Specific technical requirements for computer security

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

6.5.2 IT security assessment

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

6.6 Technical life cycle controls

6.6.1 System development controls

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

6.6.2 Security management controls

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

6.6.3 Lifecycle security controls

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

6.7 Network security controls

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

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 Certification Policy, the following types of certificates are issued, with their associated OIDs:

Type of Certificate	**OID**
Corporate Certificates for Professional Association Member. High-Level with portable QSCD	1.3.6.1.4.1.13177.10.1.1.1
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 Professional Association Member. Other devices	1.3.6.1.4.1.13177.10.1.1.2
Corporate certificates for Natural Person. High-Level with portable QSCD	1.3.6.1.4.1.13177.10.1.2.1
Corporate certificates for Natural Person. High-Level with centralised QSCD	1.3.6.1.4.1.13177.10.1.2.3
Corporate certificates for Natural Person. Other devices	1.3.6.1.4.1.13177.10.1.2.2
Corporate Certificates for Natural Person to sign emails. Other devices	1.3.6.1.4.1.13177.10.1.14.2
Corporate Certificates for Legal Representative. Within portable QSCD	1.3.6.1.4.1.13177.10.1.11.1
Corporate Certificates for Legal Representative. Within centralised QSCD	1.3.6.1.4.1.13177.10.1.11.3

Corporate Certificates for Legal Representative. Other devices	1.3.6.1.4.1.13177.10.1.11.2
Corporate Certificates for Voluntary Representative towards Public Administration. Within portable QSCD	1.3.6.1.4.1.13177.10.1.12.1
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 Voluntary Representative towards Public Administration. Other devices	1.3.6.1.4.1.13177.10.1.12.2
Corporate Certificates for Representative of Entity without Legal Personality. Within portable QSCD	1.3.6.1.4.1.13177.10.1.13.1
Corporate Certificates for Representative of Entity without Legal Personality. Within centralised QSCD	1.3.6.1.4.1.13177.10.1.13.3
Corporate Certificates for Representative of Entity without Legal Personality. Other devices	1.3.6.1.4.1.13177.10.1.13.2
Certificates for Public Servant. High-Level with portable QSCD	1.3.6.1.4.1.13177.10.1.22.1
Certificates for Public Servant. High-Level with centralised QSCD	1.3.6.1.4.1.13177.10.1.22.3
Certificates for Public Servant. Medium-Level	1.3.6.1.4.1.13177.10.1.22.2

Certificates for Public Servant with Pseudonym or with professional identification number	1.3.6.1.4.1.13177.10.1.23.2
Personal Certificates. Other devices	1.3.6.1.4.1.13177.10.1.40.2
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.

firmaprofesional