

## Certification Policy

# Electronic Seal Certificates

Version: 230216

Classification: Public



## Version history

Version	Section and changes	Date of publication
190121	<ul style="list-style-type: none"> <li>New Certification Policy for Electronic Seal Certificates that groups together all existing policies regarding this type of certificate. May be consulted at <a href="http://firmaprofesional.com/cps">http://firmaprofesional.com/cps</a></li> </ul>	21/01/2019
190507	<ul style="list-style-type: none"> <li>Homogenization of the terminology of Public Administration Seal.</li> <li>Period of validity of Public Administration Seal certificates increased from 3 to 5 years.</li> <li>Validation of applicant's email before issuing the certificate.</li> <li>Changed the CA that issues the Public Administration Seal to "AC Firmaprofesional - CUALIFICADOS".</li> </ul>	07/05/2019
190612	<ul style="list-style-type: none"> <li>Inclusion of seal certificates for payment services based on the Payment Services Directive 2015/2366 (PSD2)</li> </ul>	12/06/2019
200417	<ul style="list-style-type: none"> <li>Added measures due to COVID-19 Spanish Alarm Status</li> </ul>	17/04/2020
210217	<ul style="list-style-type: none"> <li>Adaptation to the new Law 6/2020, regulating certain aspects of electronic trust services</li> </ul>	17/02/2021
220216	<ul style="list-style-type: none"> <li>Adaptation to the RFC 3647</li> <li>General review</li> </ul>	16/02/2022
230216	<ul style="list-style-type: none"> <li>General review</li> </ul>	16/02/2023

## Index

<b>1. Introduction</b>	<b>10</b>
1.1. Summary	10
1.2. Identification of the Document	11
1.3 Participating entities	12
1.3.1. Certification Authorities (CA)	12
1.3.2. Registration Authority (RA)	12
1.3.3 Subscribers	13
1.3.3.1. Applicant	13
1.3.4 Third parties trusting in certificates	13
1.3.5. Other participants	13
1.4. Use of certificates	14
1.4.1. Appropriate use of certificates	14
1.4.1.1 Certificate Validity Period	15
1.4.2. Non authorised use of certificates	15
1.5 Policy Administration	15
1.5.1 Organization managing the document	15
1.5.2 Contact person	15
1.5.3 Person who determines the suitability of the CP for the policy	16
1.5.4 CP approval procedure	16
1.6 Definitions and acronyms	16
<b>2. Repositories and Publication of Information</b>	<b>16</b>
2.1 Repositories	16
2.2 Publication of certification information	16
2.3 Time or frequency of publication	16
2.4 Access control to repositories	17
<b>3. Identification and Authentication</b>	<b>17</b>
3.1 Registration of Names	17
3.1.1 Types of names	17
3.1.2 Need for names to be meaningful	17
3.1.3 Anonymity or pseudonymity of subscribers	17
3.1.4 Rules for interpreting various forms of names	17
3.1.5 Uniqueness of names	18
3.1.6 Recognition, authentication and role of trademarks	18
3.2 Initial validation of identity	18
3.2.1 Private key possession test method	18
3.2.2 Authentication of the organization's identity and domain identity	18
3.2.3 Authentication of the identity of a natural person	18
3.2.4 Unverified subscriber information	18
3.2.5 Validation of the identity of the RA and RA operators	19
3.2.6 Interoperability criteria	19

3.3 Identification and authentication for key renewal requests	19
3.3.1 Identification and authentication for password change	19
3.3.2 Identification and authentication for the renewal of certificates after their revocation	19
3.4 Identification and authentication for revocation request	19
<b>4. Operational requirements of the certificate life cycle</b>	<b>20</b>
4.1. Certificate request	20
4.1.1 Who can submit a certificate request	20
4.1.2 Certificate application process and responsibilities	20
4.2 Processing of certificate applications	21
4.2.1 Performing identification and authentication functions	21
4.2.2 Approval or denial of certificate applications	22
4.2.3. Processing time for certificate requests	22
4.3 Issuance of certificates	22
4.3.1 Actions of the CA during the issuance of the certificate	22
4.3.2 Notification to the subscriber by the CA of the issuance of the certificate	23
4.4 Certificate acceptance	23
4.4.1 Form in which the certificate is accepted	23
4.4.2 Publication of the certificate by the CA	24
4.4.3 Notification of the issuance of the certificate by the CA to other entities	24
4.5 Use of keys and certificate	24
4.5.1 Use of the subscriber's certificate and private key	24
4.5.2 Use of certificates and public keys by parties who trust the certificates	24
4.6. Certificate renewal without change of keys	24
4.6.1. Circumstance for the renewal of the certificate	24
4.6.2. Who can apply for renewal	24
4.6.3. Certificate renewal request process	25
4.6.4. Notification to the subscriber of the issuance of a new certificate	25
4.6.5. Conduct that constitutes acceptance of a renewal certificate	25
4.6.6. Publication of the renewal certificate by the CA	25
4.6.7. Notification of the issuance of the certificate by the CA to other entities	25
4.7 Renewal of the certificate with change of keys	26
4.7.1 Circumstance for changing the certificate key	26
4.7.2 Who can request the certification of a new public key	26
4.7.3 Processing certificate key change requests	26
4.7.4 Notification to the subscriber of the issuance of a new certificate	26
4.7.5 Conduct that constitutes acceptance of a certificate with a new key	26
4.7.6 Publication of the certificate with a new key by the CA	27
4.8 Modification of the certificate	27
4.8.1. Circumstance of the certificate modification	27
4.8.2. Who can request the modification of the certificate	27
4.8.3. Processing of certificate modification requests	27
4.8.4. Notification of the issuance of a new certificate to the subscriber	27
4.8.5. Behavior that constitutes acceptance of a modified certificate	27
4.8.6. Publication of the certificate modified by the CA	27

4.8.7. Notification of the issuance of certificates by the CA to other entities	27
4.9 Revocation and suspension of certificates	28
4.9.1 Circumstances for revocation	28
4.9.2 Who can request revocation	28
4.9.3 Revocation request procedure	28
4.9.4 Grace period for revocation request	28
4.9.5 Time within which CA must process the revocation request	28
4.9.6 Revocation verification requirement for relying parties	28
4.9.7 CRL issuance frequency	29
4.9.8 Maximum latency for CRLs	29
4.9.9 Online status check / revocation availability	29
4.9.10 Online revocation verification requirements	29
4.9.11 Other forms of revocation announcements available	29
4.9.12 Special requirements related to the key engagement	29
4.9.13 Circumstances for suspension	29
4.9.14 Who can request suspension	30
4.9.15 Suspension request procedure	30
4.9.16 Limits of the period of suspension	30
4.10 Certificate status services	30
4.10.1 Operational characteristics	30
4.10.2 Service availability	30
4.10.3 Optional functions	30
4.11 Termination of subscription	31
4.12 Custody and recovery of keys	31
4.12.1 Key custody and recovery policy and practices	31
4.12.2 Session Key Encapsulation and Recovery Policy and Practices	31
<b>5. Physical security, facilities, management and operational controls</b>	<b>32</b>
5.1 Physical controls	32
5.1.1 Site location and construction	32
5.1.2 Physical access	32
5.1.3 Energy and air conditioning	32
5.1.4 Exposure to water	32
5.1.5 Fire prevention and protection	32
5.1.6 Media storage	33
5.1.7 Waste disposal	33
5.1.8 Off-site backup	33
5.2 Procedural controls	33
5.2.1 Trusted roles	33
5.2.2 Number of people needed per task	33
5.2.3 Identification and authentication for each role	33
5.2.4 Roles requiring separation of duties	34
5.3 Personnel controls	34
5.3.1 Qualifications, experience and authorization requirements	34
5.3.2 Background check procedures	34

5.3.3 Training requirements	34
5.3.4 Retraining frequency and requirements	34
5.3.5 Frequency and sequence of job rotation	34
5.3.6 Sanctions for unauthorized actions	35
5.3.7 Requirements for independent contractors	35
5.3.8 Documentation provided to personnel	35
5.4 Audit log procedures	35
5.4.1 Types of recorded events	35
5.4.2 Frequency of processing audit records	35
5.4.3 Retention period of audit records	35
5.4.4 Protection of audit logs	36
5.4.5 Back-up procedures for audit records	36
5.4.6 Audit collection system	36
5.4.7 Notification to the subject causing the event	36
5.4.8 Vulnerability analysis	36
5.5 Log file	36
5.5.1 Types of Archived Records	36
5.5.2 File retention period	37
5.5.3 File protection	37
5.5.4 File backup procedures	37
5.5.5 Requirements for time stamping of records	37
5.5.6 File collection system	37
5.5.7 Procedures for obtaining and verifying file information	37
5.6 Password change	37
5.7 Disaster recovery plan	38
5.7.1 Incident and engagement management procedures	38
5.7.2 Computer resources, software and / or data become corrupted	38
5.7.3 Procedures for compromising the entity's private key	38
5.7.4 Business continuity capabilities after a disaster	38
5.8 Cessation of activity of the RA or CA	38
<b>6. Technical security controls</b>	<b>39</b>
6.1 Key pair generation and installation	39
6.1.1 Key pair generation	39
6.1.2 Delivery of the private key to the subscriber	39
6.1.3 Delivery of the public key to the certificate issuer	39
6.1.4 Delivery of the CA's public key to relying parties	39
6.1.5 Key size	39
6.1.6 Generation of public key parameters and quality control	40
6.1.7 Key usage purposes (depending on the field of use of the X.509 v3 key)	40
6.2 Private key protection and cryptographic module engineering controls	40
6.2.1 Cryptographic module rules and controls	40
6.2.2 Multi-person control (k of n) of the private key	40
6.2.3 Private key deposit	40
6.2.4 Private key backup	40

6.2.5 Private key file	41
6.2.6 Transfer of private keys to or from a cryptographic module	41
6.2.7 Storage of the private key in the cryptographic module	41
6.2.8 Private key activation method	41
6.2.9 Private key deactivation method	41
6.2.10 Private key destruction method	41
6.2.11 Cryptographic module classification	41
6.3 Other aspects of key pair management	42
6.3.1 Public key file	42
6.3.2 Certificate operation periods and key pair usage periods	42
6.4 Activation data	42
6.4.1 Generation and installation of activation data	42
6.4.2 Protection of activation data	42
6.4.3 Other aspects of activation data	43
6.5 IT security controls	43
6.5.1 Specific technical requirements for computer security	43
6.5.2 IT security assessment	43
6.6 Technical life cycle controls	43
6.6.1 System development controls	43
6.6.2 Security management controls	43
6.6.3 Lifecycle security controls	44
6.7 Network security controls	44
6.8 Time control	44
<b>7. Profiles of certificates, CRL and OCSP</b>	<b>45</b>
7.1 Certificate profile	45
7.1.1 Version number (s)	45
7.1.2 Certificate extensions	45
7.1.3 Algorithm object identifiers	45
7.1.4 Name forms	45
7.1.5 Name restrictions	45
7.1.6 Certificate policy object identifier	46
7.1.7 Using the Policy Constraints extension	46
7.1.8 Syntax and semantics of policy qualifiers	46
7.1.9 Processing semantics of the critical Certificate Policies extension	46
7.2 CRL profile	47
7.2.1 Version number (s)	47
7.2.2 CRL extensions and CRL entries	47
7.3 OCSP profile	47
7.3.1 Version number (s)	47
7.3.2 OCSP extensions	47
<b>8. Compliance audits and other controls</b>	<b>48</b>
8.1 Frequency of audits	48
8.2 Qualification of the auditor or evaluator	48
8.3 Relationship between the auditor and the audited authority	48



8.4 Aspects covered by the evaluation	48
8.5 Actions to be taken as a result of the detection of deficiencies	48
<b>9. Other legal and business issues</b>	<b>49</b>
9.1 Fees	49
9.1.1 Certificate issuance or renewal fees	49
9.1.2 Fees for access to certificates	49
9.1.3 Access fees to revocation or status information	49
9.1.4 Fees for other services	49
9.1.5 Refund fees	50
9.2 Financial responsibilities	50
9.2.1 Insurance coverage	50
9.2.2 Other assets	50
9.2.3 Insurance or guarantee coverage for end entities	50
9.3 Confidentiality of commercial information	50
9.3.1 Scope of confidential information	50
9.3.2 Non-confidential information	50
9.3.3 Responsibility to protect confidential information	51
9.4 Protection of personal information	51
9.4.1 Personal data protection policy	51
9.4.2 Information treated as private	51
9.4.3 Information not considered private	51
9.4.4 Responsibility to protect private information	51
9.4.5 Notice and consent to the use of private information	51
9.4.6 Disclosure under judicial or administrative process	52
9.4.7 Other information disclosure circumstances	52
9.5 Intellectual property rights	52
9.6 Obligations and guarantees	52
9.6.1 Obligations of the CA	52
9.6.2 Obligations of the RA	52
9.6.3 Obligations of applicants	52
9.6.4 Representations and guarantees of third parties who trust the certificates	53
9.6.5 Representations and guarantees of other participants	53
9.7 Disclaimer of warranty	53
9.8 Limitations of liability	53
9.9 Indemnification	53
9.10 Period of validity and termination	53
9.10.1 Term	53
9.10.2 Termination	54
9.10.3 Effect of termination and survival	54
9.11 Notices and individual communications with participants	54
9.12 Modifications or changes in specifications	54
9.12.1 Procedure for changes	54
9.12.2 Notification mechanism and deadline	54
9.12.3 Circumstances in which the OID must be modified	54



9.13 Provisions for conflict resolution	55
9.14 Applicable regulations	55
9.15 Cumplimiento de la normativa aplicable	55
9.16 Disposiciones diversas	55
9.16.1 Acuerdo completo	55
9.16.2 Independencia	55
9.16.3 Resolución por vía judicial	55
9.16.4 Ejecución (honorarios de abogados y renuncia de derechos)	56
9.16.5 Fuerza mayor	56
9.17 Otras disposiciones	56

# 1. Introduction

## 1.1. Summary

Firmaprofesional issues this Certification Policy for Electronic Seal Certificates, grouping together distinct policies that define certificates intended to sign, on behalf of the organization or body, electronic documents automatically under the responsibility of the certificate subscriber.

This document defines the Certification Policies for the following certificates:

1. Certificates for Seals of Public Administration (Administration, Body or Public Legal Entity).
2. Corporate Certificates for Company Seal.
3. Certificates for Electronic Seal for payment services (certificates for electronic seal for PSD2).

Electronic Seal Certificates are issued in accordance with Annex III of Regulation EU 910/2014, which specifies the requirements for qualified electronic seal certificates, and defines them as “an electronic statement that links the validation data of a seal with a legal person and confirms their identity”. The objective of an electronic seal is to guarantee the origin and integrity of data. They are used to identify an entity (either public or private) or a Public Administration Body, and to automatically sign on behalf of that entity or body.

Spanish regulations require that distinction be made between:

- **Certificates for Seals of Administration, Body or Public Right Entity:** qualified certificates issued to Public Administrations, Bodies or Public Right Entities for devices, in accordance with indications of article 40 of Law 40/2015, 1st October, of Public Sector Legal Regime.
- **Corporate Certificates for Company Seal:** qualified digital certificates, issued in accordance with Law 6/2020 LSEC, that identify both subscriber and signatory as a Corporation with Legal Personality. These certificates adapt to requirements of Law 25/2013, 27th December, for enhancement of electronic invoicing and creation of invoice accounting register for Public Sector, and have been authorised, amongst

other uses, for their use in electronic invoicing and digitalisation certified by the Tax Agency.

- **Certificates for Electronic Seal for PSD2:** qualified electronic certificates used to identify the payment service provider and provide evidence of authenticity and integrity of the sealed data.

Specific conditions regarding this type of certificates are defined in this document. This Certification Policy (hereafter “CP”) is subject to compliance with the Certification Practices Statement (hereafter “CPS”) of Firmaprofesional.

## 1.2. Identification of the Document

<b>Name:</b>	Certification Policy for Electronic Seal Certificates
<b>Version:</b>	230216
<b>Description:</b>	Development of a Certification Policy for Electronic Seal Certificates including both Certificates for Company Seal and Certificates for Seal of Administration, Body or Public Right Entity and Seal Certificates for PSD2
<b>Issuance date:</b>	16/02/2023
<b>OIDs</b>	1.3.6.1.4.1.13177.10.1.21.D (*) Seal for Administration, Body or Public Right Entity.  1.3.6.1.4.1.13177.10.1.10.D (*) Company Seal and electronic seal certificates for PSD2.
<b>Location:</b>	<a href="http://www.firmaprofesional.com/cps">http://www.firmaprofesional.com/cps</a>

(\*)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:

- Certification Policy for Certificates for Seal of Administration, Body or Public Legal Entity. Version 171121. This Policy may be consulted at <https://www.firmaprofesional.com/cps>, section “Previous Certification Policies and Practices” .

- Certification Policy for Corporate Certificates for Company Seal. Version 171121. This Policy may be consulted at <https://www.firmaprofesional.com/cps>, section “Previous Certification Policies and Practices”.

## 1.3 Participating entities

### 1.3.1. Certification Authorities (CA)

Certificates must be issued by Firmaprofesional as Trust Services Provider that issues recognised certificates according to Law 6/2020, of November 11, regulating certain aspects of electronic trust services (hereinafter Law 6/2020 LSEC), and qualified certificates in accordance with Regulation EU 910/2014 (eIDAS).

Specifically, CA issuing certificates, depending on the type, are:

- Certificates for Company Seal and Certificates for Seal of Administration, Body or Public Right Entity are issued by “AC Firmaprofesional - CUALIFICADOS”.

### 1.3.2. Registration Authority (RA)

Management of applications and issuances shall be performed by entities acting as Registration Authorities of Firmaprofesional.

Each entity acting as RA of Firmaprofesional will 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.

### 1.3.3 Subscribers

The certificate subscriber will be the entity identified in the Certificate.

The subscriber of the PSD2 electronic seal certificate will be the payment service provider duly authorized and registered in the public registry of the Competent National Authority. The subscriber will always be a legal person included, at least, in one of the following categories:

- Account manager
- Payment initiation service provider
- Account information provider
- Issuer of card-based payment instruments.

#### 1.3.3.1. Applicant

The following certificates may be requested:

- Public Administration Seal Certificates: any person authorized by the Administration, Body or Public Right Entity.
- Company Seal Certificates: entity administrator, legal representative, person empowered by power of attorney for this purpose or any person authorized by one of the already mentioned.

### 1.3.4 Third parties trusting in certificates

Third parties trusting in certificates shall acknowledge their usage limitations, established in the CPS and in this CP.

Certificates are recognised by @firma, Validation and Electronic Signature Platform of Spanish Government.

### 1.3.5. Other participants

Without stipulation.

## 1.4. Use of certificates

### 1.4.1. Appropriate use of certificates

Certificates may be used in accordance with terms established in the CPS and by the regulation in force.

Specifically, the appropriate use of each certificate is as follows:

- Certificates for Public Administration Seal: These certificates may be used as an identification and authentication mechanism in electronic signature systems for automated administrative action.
- Certificates for Company Seal: These certificates may be used for authentication in secure communication systems, remission of commercial communications, publication of information on the company website, etc. Valid for their use in electronic invoicing and certified digitalisation. They adapt to requirement of Law 25/2013, 27th December, for enhancement of electronic invoicing and creation of invoice accounting register for Public Sector, and have been authorised for their use in electronic invoicing and digitalisation certified by the Tax Agency.
- Certificates for Electronic Seal for PSD2: These certificates can be used to allow account information service providers, payment initiation service providers and payment service providers that issue card-based payment tools, the identification of themselves to the payment services provider that is account manager.

### 1.4.1.1 Certificate Validity Period

The validity period will be as indicated within the certificate itself, with the following limitations:

Profile	Other devices / Medium-Level	QSCD / High-Level
Public Administration Seal	Up to a maximum of 5 years	Up to a maximum of 5 years
Company Seal	Up to a maximum of 5 years	-
Electronic Seal for PSD2	Up to a maximum of 5 years	-

### 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.

## 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 Access control to repositories

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

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

### 3.1.3 Anonymity or pseudonymity of subscribers

Without stipulation.

### 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 the Firm profesional.

### **3.1.6 Recognition, authentication and role of trademarks**

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

## **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**

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

### **3.2.5 Validation of the identity of the RA and RA 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. Operational requirements of the certificate life cycle

### 4.1. Certificate request

Firmaprofesional will only accept applications that are manually or electronically signed by the applicant and that meet the requirements established for each type of certificate.

#### 4.1.1 Who can submit a certificate request

Applications for these certificates will be made by legal representatives or persons empowered by power of attorney of the Holder of the Electronic Seal duly accredited and authorized to do so or by those persons authorized by legal representatives or persons empowered by power of attorney.

#### 4.1.2 Certificate application process and responsibilities

The steps to follow to obtain the certificate are detailed below:

The applicant must contact Firmaprofesional directly, providing all the necessary documentation to verify the identity of the legal entity.

In the case of request for Public Administration Seal certificates, Firmaprofesional will verify that:

- There is a resolution of the Undersecretariat of the Ministry or head of the competent public body by which the Electronic Seal is created and is published in the corresponding Electronic Headquarters, in the event that the law requires it.
- The data of the request for the Electronic Seal certificate coincide with the data published in the Resolution, in the event that the law requires such resolution.

In case of requesting HIGH level, evidence must be provided that the generation and custody of keys is carried out in a cryptographic hardware device approved by the Ministry responsible for information society services.

Firmaprofesional will verify the status of legal representative or person empowered by power of attorney for the request for the Business Seal certificates either by telematic consultation with the Commercial Registry or by reviewing the notarial or legal documentation provided by the applicant. The legal representative of the entity may authorize a person from the entity as an applicant for the Business Seal certificates, and who will be the person responsible for their control and management, as well as for their proper use. For this, the applicant must provide a document from the legal representative, where the applicant is expressly authorized to request the business seal certificate, attaching a copy of the authorizing identity document and their powers of representation, or in PDF format signed electronically with their valid legal representative certificate.

In cases where Firmaprofesional has previously verified the identity of the Legal Person and the applicant, it will not be necessary to carry out additional verifications. Specific:

- If the applicant has a valid Corporate Legal Representative Certificate issued by Firmaprofesional.
- If the Corporation acts as RA of Firmaprofesional for the issuance of its own certificates.

In case of request for electronic seal certificates for PSD2, the payment service provider will submit the request together with the certificate of being a payment service provider authorized by the Competent National Authority, together with the authorization number, the role of the provider. of the payment service and the name of the Competent National Authority of the place where the payment service provider is registered. The request for issuance of the electronic seal certificate for PSD2 must be signed by a natural person who represents the payment service provider and who is recorded as such in the Competent National Authority.

## **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 signer. This process must be carried out prior to the issuance of the certificate.

## 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 Issuance of certificates

### 4.3.1 Actions of the CA during the issuance of the certificate

Each Firmaprofesional Registration Authority will have accredited a series of people to act as RA Operator against Firmaprofesional. The RA Operators will have been authorized to perform this function and will have been previously instructed in the operation of issuing certificates.

Processing phases are as follows:

#### 1. Keys generation

The RA Operator will validate the veracity and accuracy of the signatory and applicant data.

In the case of electronic seal certificates for PSD2, the RA operator will validate the information presented by the payment service provider by comparing it with the information available in the Public Registry of the National Competition Authority.

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.

#### 2. 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.

### **3. 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.

#### **4.3.2 Notification to the subscriber by the CA of the issuance of the certificate**

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 Publication of the certificate 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 certificates and public keys by parties who trust the certificates**

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

### **4.6. Certificate renewal without change of keys**

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

#### **4.6.1. Circumstance for the renewal of the certificate**

Without stipulation.

#### **4.6.2. Who can apply for renewal**

Without stipulation.

#### **4.6.3. Certificate renewal request process**

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 Renewal of the certificate with change of keys**

### **4.7.1 Circumstance for changing the certificate key**

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

### **4.7.2 Who can request the certification of a new public key**

The subscriber must go to his RA, and proceed to the generation of a new certificate.

### **4.7.3 Processing certificate key change requests**

In the case of Business Seal certificates, their renewal can be done online as long as the RA has the service and the subscriber has contracted the renewal. In this case, the subscriber will receive a notification from the RA by email to initiate the renewal through the Firmaprofesional website.

The validity period of certificates renewed online will be conditioned by the requirements established in article 7 of Law 6/2020 LSEC.

The renewal of the Electronic Seal certificates for PSD2 necessarily implies a new verification of all the attributes of the payment service provider, as was done in the initial issuance.

### **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**

#### **4.8.1. Circumstance of the certificate modification**

Without stipulation.

#### **4.8.2. Who can request the modification of the certificate**

Without stipulation.

#### **4.8.3. Processing of certificate modification requests**

Without stipulation.

#### **4.8.4. Notification of the issuance of a new certificate to the subscriber**

Without stipulation.

#### **4.8.5. Behavior that constitutes acceptance of a 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 certificates 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 issuance 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 status check / revocation 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 period of suspension**

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 Retraining frequency and requirements**

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 of 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 (s)

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
High-Level Certificate of Seal for Public Administration issued in a portable QSCD	1.3.6.1.4.1.13177.10.1.21.1
High-Level Certificate of Seal for Public Administration issued in a centralised QSCD	1.3.6.1.4.1.13177.10.1.21.3
Medium-Level certificate of Seal for Public Administration issued in other devices	1.3.6.1.4.1.13177.10.1.21.2
Company Seal Certificate and PSD2	1.3.6.1.4.1.13177.10.1.10.2

### 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 (s)

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 (s)

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 Fees

Firmaprofesional will charge the Subscriber what is agreed in the service provision contract signed by the parties.

Firmaprofesional may establish the rates it deems appropriate for subscribers, as well as establish the means of payment it deems most appropriate in each case. For more details on the price and payment conditions of this type of certificate, it will be necessary to consult with the Commercial Department of Firmaprofesional.

#### 9.1.1 Certificate issuance or renewal fees

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

#### 9.1.2 Fees for access to certificates

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

#### 9.1.3 Access fees to revocation or status information

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 Refund 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 Cumplimiento de la normativa aplicable**

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

### **9.16 Disposiciones diversas**

#### **9.16.1 Acuerdo completo**

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

#### **9.16.2 Independencia**

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

#### **9.16.3 Resolución por vía judicial**

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

#### **9.16.4 Ejecución (honorarios de abogados y renuncia de derechos)**

Sin estipulación.

#### **9.16.5 Fuerza mayor**

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

#### **9.17 Otras disposiciones**

Sin estipulación.