

## Certification Policy

# Electronic signatures certificates

Version: 190507

Classification: Public



## Version history

Version	Section and changes	Date of publication
190121	<ul style="list-style-type: none"><li>• New Certification Policy for Personal 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>• Added verification of the applicant's email before the issuance of the certificate.</li><li>• Restructured the OIDs, eliminating duplicities.</li><li>• Error correction.</li><li>• Changed the CA that issues the Public Servant certificates to "AC Firmaprofesional - CUALIFICADOS".</li></ul>	07/05/2019

# Index

<b>1. Introduction</b>	<b>4</b>
1.1. General Description	4
1.2. Identification of the Document	5
<b>2. Participating Entities</b>	<b>7</b>
2.1. Trust Services Provider (TSP)	7
2.2. Registration Authorities (RA)	7
2.3. Applicant	8
2.4. Subscriber	9
2.5. Signatory	9
2.6. Third parties trusting in certificates	10
<b>3. Certificate Features</b>	<b>10</b>
3.1. Certificate Validity Period	10
3.2. Signature Creation Devices	10
3.3. Specific use of certificates	11
3.3.1. Appropriate use of certificates	11
3.3.2. Non authorised use of certificates	11
3.3.3. Rates	12
<b>4. Operational procedures</b>	<b>12</b>
4.1. Certificate issuance process	12
4.1.1 Application	12
4.1.2 Application acceptance	13
4.1.3 Processing	14
4.2. Certificate revocation	16
4.3. Certificate renewal	16
<b>5. Certificate profiles</b>	<b>17</b>

# 1. Introduction

## 1.1. General Description

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 59/2003, 19th December for Electronic Signature (hereafter “Law 59/2003”), and Qualified Certificates in compliance with requirements established in Annex I of 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

<b>Name:</b>	CP Electronic Signature Certificates
<b>Version:</b>	190507
<b>Description:</b>	Certification Policy for Electronic Signature Certificates where all certificates issued to natural persons (with and without attributes) are grouped together.
<b>Date of Issuance:</b>	07/05/2019

<b>OIDs:</b>	<p>1.3.6.1.4.1.13177.10.1.1.D (*) Certificates for Professional Association Member</p> <p>1.3.6.1.4.1.13177.10.1.2.D (*) Corporate Certificates for Natural Person</p> <p>1.3.6.1.4.1.13177.10.1.11.D (*) Corporate Certificates for Legal Representative</p> <p>1.3.6.1.4.1.13177.10.1.12.D (*) Corporate Certificates for Voluntary Representative towards Public Administration</p> <p>1.3.6.1.4.1.13177.10.1.13.D (*) Corporate Certificates for Representative of Entity without Legal Personality</p> <p>1.3.6.1.4.1.13177.10.1.22.D (*) Certificate for Public Servant</p> <p>1.3.6.1.4.1.13177.10.1.23.D (*) Certificate for Public Servant with pseudonym</p> <p>1.3.6.1.4.1.13177.10.1.40.D (*) Personal Certificates</p>
<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:

- 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”.

## 2. Participating Entities

### 2.1. Trust Services Provider (TSP)

All certificates described in this Policy must be issued by Firmaprofesional as Trust Services Provider that issues recognised certificates according to Law 59/2003, and qualified certificates in accordance with Regulation EU 910/2014.

Corporate certificates, personal certificates and public servant certificates are issued by the Subordinate Certification Authority (CA) “AC Firmaprofesional - CUALIFICADOS”.

### 2.2. 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.

## 2.3. Applicant

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

## 2.4. Subscriber

The subscriber is the natural or legal person that hires the trust services of Firmaprofesional, and therefore shall be the owner of the certificate. As a result, the subscriber shall have the revocation and suspension rights of the certificate.

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

- The Professional Association in cases of Certificates for Professional Association Member.
- The Corporation in cases of Corporate Certificates for Natural Person and Legal Person (all types, Entity without Legal Personality, Legal Representative and Voluntary Representative towards Public Administration).
- The applicant themselves, in cases of Certificates for Natural Person.
- The Administration, Body or Public-Law Entity in cases of Certificates for Public Servant and Public Servant with pseudonym.

## 2.5. 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 person shall be identified by a pseudonym.

## 2.6. Third parties trusting in certificates

All certificates described in this Policy are recognised certificates that comply with requirements established in Signature Electronic Law.

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.

## 3. Certificate Features

### 3.1. Certificate Validity Period

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

### 3.2. Signature Creation 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 article 24 of Law 59/2033 and Annex II of Regulation EU 910/2014, 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 .

### 3.3. Specific use of certificates

#### 3.3.1. 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.

#### 3.3.2. 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.

### **3.3.3. 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 Commercial Department of Firmaprofesional should be consulted.

## **4. Operational procedures**

### **4.1. Certificate issuance process**

Steps to obtain a certificates are as follows:

#### **4.1.1 Application**

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 or without pseudonym), 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 Organisation 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.

#### **4.1.2 Application acceptance**

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:
  - o Online consultation with Trade Registry.
  - o Revision of the notarial documentation provided.
  - o 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.

### **4.1.3 Processing**

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 QSCD that will allow them to manage users applications.

In case of Personal Certificates, once the application is approved, and prior to the issuance of the certificate, Firmaprofesional will check the validity of the email provided by the applicant, sending an email with a 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 they 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 validate the veracity and accuracy of the signatory data. For this, and prior to the issuance of the certificate, Firmaprofesional will check the validity of the email provided by the applicant, sending an email with a random data, which the applicant must access to prove the existence of that email account.

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 13 of Law 59/2003, 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 13 of Law 59/2003.

## 4.2. Certificate revocation

In accordance with specifications of the Certification Practices Statement (CPS).

## 4.3. Certificate renewal

The following procedures apply:

1. In person: the signatory must present themselves in person towards the RA of Firmaprofesional and apply for a new certificate.
2. Online: if the RA has such service, the signatory must connect to the online service that Firmaprofesional provides with their current certificate still in force and electronically sign the renewal application, or they need to have another mechanism



that allows to authenticate their identity and the will to renew the certificate. Possibility to perform the renewal online is subject to requirements of current legislation. The validity period of the certificate renewed online is subject to requirements established within article 13 of Law 59/2003.

3. Automatic (only available for Personal Certificates): if the signatory accepts this possibility at the time of issuance, before expiry of current certificate a new certificate will be automatically generated with the same keys. Possibility for performing a automatic renewal is subject to conditions established in the current legislation.

## 5. Certificate profiles

The following types of certificates are issued under the prescriptions contained in this Certification Policy, 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 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	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

Extensions used for each type of certificate issued under this policy are published in the document titled "Certificate Profiles of Firmaprofesional" located on the Firmaprofesional website (<http://www.firmaprofesional.com/cps>).



Firmaprofesional, S.A.

May 2019