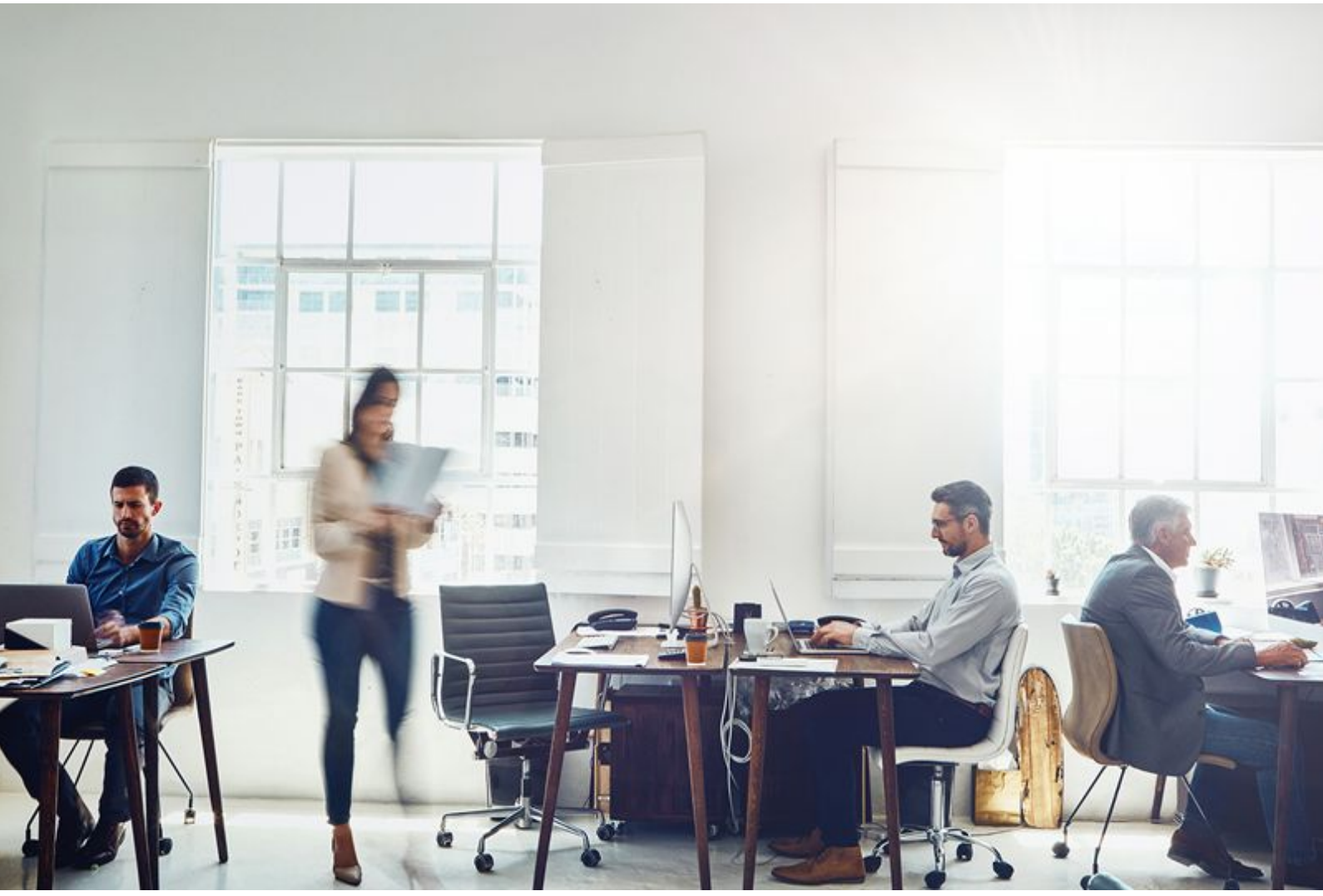
Certification Policy

Electronic Seal Certificates

Version: 190507

Classification: Public



BARCELONA
EDIF. ESADECREAPOLIS
AV. TORRE BLANCA, 57 - LOCAL M2
08173 SANT CUGAT DEL VALLÈS
+34 934 774 245

MADRID
VELÁZQUEZ 59, 1º CTRO.-IZDA.
28001 MADRID
+34 915 762 181

WWW.FIRMAPROFESIONAL.COM

Version history

Version	Section and changes	Date of publication
190121	• New Certification Policy for Electronic Seal Certificates that groups together all existing policies regarding this type of certificate. May be consulted at http://firmaprofesional.com/cps	21/01/2019
190507	• Homogenization of the terminology of Public Administration Seal. • Period of validity of Public Administration Seal certificates increased from 3 to 5 years. • Validation of applicant's email before issuing the certificate. • Changed the CA that issues the Public Administration Seal to "AC Firmaprofesional - CUALIFICADOS".	07/05/2019

Index

1. Introduction **4**

1.1. General description 4

1.2. Identification of the Document 5

2. Participating entities **6**

2.1. Certification Authorities (CA) 6

2.2. Registration Authority (RA) 6

2.3. Applicant 6

2.4. Subscriber 7

2.5. Third parties trusting in certificates 7

3. Certificate features **7**

3.1. Certificate Validity Period 7

3.2. Specific use of certificates 8

3.2.1. Appropriate use of certificates 8

3.2.2. Non authorised use of certificates 8

3.3. Rates 8

4. Operations procedures **9**

4.1. Certificate issuance process 9

4.2. Certificate revocation 11

4.3. Certificate renewal 11

5. Certificate profiles **12**

1. Introduction

1.1. General description

Firmaprofesional issues this Certification Policy for Electronic Seal Certificates, grouping together distinct policies that defines 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.

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 59/2003, 19th December, of Electronic Seal, 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.

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

Name:	Certification Policy for Electronic Seal Certificates
Version:	190507
Description:	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.
Issuance date:	07/05/2019
OIDs	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.
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:

- 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".

2. Participating entities

2.1. Certification Authorities (CA)

Certificates must be issued by Firmaprofesional as Trust Services Provider that issues recognised certificates according to Law 59/2003 of Electronic Signature, and qualified certificates in accordance with Regulation EU 910/2014.

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".

2.2. 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.

2.3. Applicant

The following certificates may be requested:

- Public Administration Seal Certificates: any person authorised by the Administration, Body or Public Right Entity.

- Company Seal Certificates: entity administrators, legal representatives and voluntary representatives empowered for this purpose.

2.4. Subscriber

The subscriber of the certificate shall be the entity identified within the certificate.

2.5. 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.

3. Certificate features

3.1. 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	_

3.2. Specific use of certificates

3.2.1. 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:

1. **Certificates for Public Administration Seal:** These certificates may be used as an identification and authentication mechanism in electronic signature systems for automated administrative action.

2. **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.

3.2.2. 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.

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. Operations procedures

4.1. Certificate issuance process

Steps to obtain a certificates are as follows:

a. Application

Applicant must contact directly Firmaprofesional, while providing all the necessary documentation in order to verify the identity of the legal person.

In case of application of Certificates for Seal of Public Administration, Firmaprofesional will verify that:

- Electronic Office exists and corresponds to data published within its Resolution of creation.
- It there exists a Resolution of the Ministry Undersecretary or holder of the competent public body by which the Electronic Seal is created, and it is published in the corresponding Electronic Office.
- Data of the application for Electronic Seal certificate coincide with data published within the Resolution.
- The application is performed by a representative of the Electronic Seal Holder, duly accredited and authorised for this purpose.

Where High-Level is applied for, evidence confirming that key generation and custody are performed within a cryptographic device approved by the corresponding Ministry is provided.

Firmaprofesional shall verify legal or voluntary representative condition for Company Seal Certificates applications, either online consultation with the Trade Register or reviewing the notarial documentation provided by the applicant.

For cases where Firmaprofesional has already verified the identity of the Legal Person and the applicant, no additional verifications will be needed. Specifically:

- If the applicant has a Corporate Certificate for Legal Representative in force issued by Firmaprofesional.
- If the Corporation acts as an RA of Firmaprofesional for their own certificates issuance.

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.

b. Application acceptance.

Firmaprofesional will only accept applications signed by hand or electronically by the subscriber, and that comply with requirements established for each type of certificate.

c. 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.

Processing phases are as follows:

1. **Keys generation**

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

   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 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.

4.2. Certificate revocation

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

4.3. Certificate renewal

Subscriber must refer to their RA and proceed to generate a new certificate.

For cases of Company Seal Certificates, renewal may be performed online as long as the RA has such a service and the subscriber has contracted the renewal. In this case, the subscriber will receive an email notification from the RA in order to start the renewal through Firmaprofesional website.

Validity period of certificates renewed online will be subject to requirements established by Law 59/2003, article 13.4.

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
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	1.3.6.1.4.1.13177.10.1.10.2

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

Firmaprofesional, S.A.

May 2019