



CORPORATE CERTIFICATE FOR NATURAL PERSONS

Certificate Policy

Version: 171121
Classification: Public

ATTENTION: The current version of this document may be found in electronic format on the Firmaprofesional website: <https://www.firmaprofesional.com/cps>

Version History

Version	Section and changes	Publication date
6.0	Initial version	15/04/2014
171121	Change of template and version numbering, starting to follow the format YYMMDD (year, month and day of publication) Inclusion of this paragraph. Adaptation to eIDAS. Added Centralized Qualified Electronic Signature Creation Device (QSCD)	21/1/2017

Index

1. INTRODUCTION	5
1.1. GENERAL DESCRIPTION	5
1.2. IDENTIFICATION OF THE DOCUMENT	5
2. PARTICIPANT ENTITIES	6
2.1. TRUST SERVICE PROVIDER (TSP)	6
2.2. REGISTRATION AUTHORITY (RA)	6
2.3. PLACE OF PERSONAL VERIFICATION	6
2.4. APPLICANT	7
2.5. SUBSCRIBER	7
2.6. SIGNER	7
2.7. PARTIES RELYING ON THE CERTIFICATES	7
3. CHARACTERISTICS OF THE CERTIFICATES	8
3.1. PERIOD OF VALIDITY OF THE CERTIFICATES	8
3.2. ELECTRONIC SIGNATURE CREATION DEVICES	8
3.3. PRIVATE USE OF CERTIFICATES	8
3.3.1. Appropriate uses of the certificates	8
3.3.2. Unauthorized use of certificates	9
3.4. TARIFFS	9
4. OPERATING PROCEDURES	10
4.1. PROCESS FOR ISSUING CERTIFICATES	10
4.2. CERTIFICATE REVOCATION	12
4.3. RENEWAL OF CERTIFICATES	12
5. CERTIFICATE PROFILE	13
5.1. DISTINGUISHED NAME (DN)	13
5.2. COMMON CERTIFICATE EXTENSIONS	14

5.3. EXTENSIONS OF THE CERTIFICATES WITHOUT QSCD	15
5.4. EXTENSIONS OF THE CERTIFICATES WITH QSCD	15

1. INTRODUCTION

1.1. GENERAL DESCRIPTION

Corporate Certificates for Natural Persons are recognized certificates of a natural person according to Law 59/2003, December 19, on Electronic Signatures that identifies the subscriber as a Corporation and the signer as associated to that Corporation, whether it be as an employee, associate, partner or supplier.

Corporate Certificates for Natural Persons are qualified certificates since they meet the requirements set out in Annex I of the EU Regulation 910/2014.

The application for and issuance of these certificates can be made through the corporations themselves to whom each certificate is linked, they act as Registration Authorities of Firmaprofesional. However, other entities, not related to the signer, that are Firmaprofesional Registration Authorities may also be used.

In the current document the special conditions concerning this type of certificate are set out. This Certificate Policy (henceforth "CP") complies with the Certification Practices Statement (henceforth the "CPS") of Firmaprofesional, which is incorporated here by reference.

1.2. IDENTIFICATION OF THE DOCUMENT

Name:	CP Corporate Certificates for Natural Persons
Version:	171121
Description:	Certification Policy for Corporate Certificates for Natural Persons
Date of Issue:	21/11/2017
OIDs	1.3.6.1.4.1.13177.10.1.2.1 (on portable QSCD) 1.3.6.1.4.1.13177.10.1.2.3 (on centralized QSCD) 1.3.6.1.4.1.13177.10.1.2.2 (on other devices)
Location	http://www.firmaprofesional.com/cps

Previously, these Certification Policies were known as:

- Type II.A - RECOGNISED CERTIFICATES OF PERSONS ASSOCIATED WITH A QSCD (1.3.6.1.4.1.13177.10.1.2.1)
- Type II.B - RECOGNISED CERTIFICATES OF ASSOCIATED PERSONS (1.3.6.1.4.1.13177.10.1.2.2)
- RECOGNISED CERTIFICATES OF ASSOCIATED PERSONS IN HARDWARE (1.3.6.1.4.1.13177.10.1.2.1)
- RECOGNISED CERTIFICATES OF ASSOCIATED PERSONS IN SOFTWARE (1.3.6.1.4.1.13177.10.1.2.2)

2. PARTICIPANT ENTITIES

2.1. TRUST SERVICE PROVIDER (TSP)

These certificates must be issued by Firmaprofesional as a Trust Service Provider issuing recognized certificates pursuant to Law 59/2003 on Electronic Signatures and qualified according to EU Regulation 910/2014.

2.2. REGISTRATION AUTHORITY (RA)

The management of the applications and issuance of the certificates will be performed by entities who act as Registration Authorities of Firmaprofesional.

In addition, the Corporation itself (companies, private or public entities) may act as a Registration Authority of Firmaprofesional for the management of the applications and issuance of certificates to those natural persons with whom it has a direct link, such as employees, partners, customers , etc...

The Corporation itself will be the subscriber of all certificates in this way.

Each corporation which acts as an RA will specify:

- The criteria which must be met when requesting a certificate, without contradicting with the provisions of the CPS and this CP.
- The mechanisms and procedures required for the identification and authentication of the signer, complying with the provisions of the CPS and this CP.
- The electronic signature creation devices to be used, chosen from among those previously approved by Firmaprofesional.

2.3. PLACE OF PERSONAL VERIFICATION

Where the geographical location of subscribers represents a logistical problem for their identification as well as in the application for and delivery of certificates, the RA may delegate these functions to a trusted entity. This entity should have a special relationship with the RA and a close relationship with the subscribers to the certificates which justifies the delegation.

For example, a Guild could act as a trusted entity for an employer, which itself acts as a Firmaprofesional RA, in the identification and delivery of certificates to companies belonging to that Guild.

The trusted entity must sign a collaboration agreement with the RA in which the delegation of these functions is accepted. Firmaprofesional must previously and expressly authorize the model agreement to be signed.

2.4. APPLICANT

The issue of a corporate certificate for a natural person may be requested by:

- The legal or voluntary representative of the Corporation, or an authorized person, on behalf of employees or persons connected with the said Corporation.
- Anyone linked to a corporation which acts as an RA of Firmaprofesional, according to the criteria established by the Corporation itself.
- Self-employed professionals or individual businessmen. In this case, in the absence of a legal person to represent them, they may request a Corporate Certificate for a Natural Person in which the identity of the natural person and legal person are the same.

2.5. SUBSCRIBER

The Corporation is the Subscriber of the certificates and, therefore, the owner of the issued certificates.

2.6. SIGNER

The signer will be the natural person identified by name, surnames, NIF (Tax Identity Number) and position within the organization. The signer must have a special relationship (employee, partner, etc) with the Corporation subscribing to certificate, so allowing the identity of the signer to be guaranteed.

The signer is the natural person who creates the electronic signature.

2.7. PARTIES RELYING ON THE CERTIFICATES

These certificates are recognized certificates that meet the requirements stipulated by the law on Electronic Signatures.

Parties relying on these certificates must be aware of the limitations in their use, both quantitative and qualitative, which are specified in the CPS and this CP.

3. CHARACTERISTICS OF THE CERTIFICATES

3.1. PERIOD OF VALIDITY OF THE CERTIFICATES

The period of validity will be as specified in the certificate itself, with a maximum of 5 years.

3.2. ELECTRONIC SIGNATURE CREATION DEVICES

In cases where Firmaprofesional can ensure that the cryptographic keys of the signer have been created on a **portable** Qualified Electronic Signature Creation Device (QSCD), in compliance with the requirements set out in Article 24 of the Law 59/2003, of 19 December, on Electronic Signatures and Annex II of the EU Regulation 910/2014 this condition will be indicated on the certificate itself using the following fields:

- "Certificate Policies" extension with OID value "1.3.6.1.4.1.13177.10.1.2.1"
- QcStatement extension with the value "id-etsi-qcs-QcSSCD" enabled

In cases where Firmaprofesional can ensure that the cryptographic keys of the signer have been created on a **centralized** Qualified Electronic Signature Creation Device (QSCD), in compliance with the requirements set out in Article 24 of the Law 59/2003, of 19 December, on Electronic Signatures and Annex II of the EU Regulation 910/2014 this condition will be indicated on the certificate itself using the following fields:

- "Certificate Policies" extension with OID value "1.3.6.1.4.1.13177.10.1.2.3"
- QcStatement extension with the value "id-etsi-qcs-QcSSCD" enabled

In any other case the condition will be indicated on the certificate itself using the following fields:

- "Certificate Policies" extension with OID value "1.3.6.1.4.1.13177.10.1.2.2"
- QcStatement extension with the value "id-etsi-qcs-QcSSCD" disabled.

3.3. PRIVATE USE OF CERTIFICATES

3.3.1. Appropriate uses of the certificates

The certificates issued by Firmaprofesional may be used under the terms established by current regulations applicable to electronic signatures, with the additional conditions set out in the CPS and this CP.

These certificates issued according to the present CP can be used for the following purposes:

- To identify the signer and their association with the corporation.
- To guarantee the integrity of the signed document.

- To identify the signer of the document.

The use of these certificates in relations between the signer and public authorities and for strictly private uses is permitted.

3.3.2. Unauthorized use of certificates

Any use that is contrary to Spanish and European Union regulations, international agreements ratified by the Spanish state, customs, morals and public order is not allowed. Use other than set out in this CP and in the CPS is also not allowed.

Using a certificate for document encryption is not recommended.

3.4. TARIFFS

Firmaprofesional will charge the Subscriber (Corporation) according to the agreement specified in the contract to provide services signed by the parties.

Firmaprofesional will set the rates which it deems appropriate to subscribers, as well as specifying the methods of payment deemed most appropriate in each case. For more details about the price and terms of payment for this type of certificate the Commercial Department of Firmaprofesional should be consulted.

4. OPERATING PROCEDURES

4.1. PROCESS FOR ISSUING CERTIFICATES

The steps for obtaining the certificate are as follows:

a) **Application**

The Corporations who act as an RA of Firmaprofesional may directly process the applications and proceed with issuing certificates to its users by accessing the Firmaprofesional system for the management and issuance of certificates. In this case, the user who wishes to apply for a certificate should contact the Corporation and make the application in the manner specified by that Corporation.

Alternatively applications for these certificates may be made directly to Firmaprofesional via any employee acting as an RA of Firmaprofesional.

b) **Acceptance of the application**

The Corporation which acts as an RA may specify the requirements that users must satisfy. The Corporation which acts as an RA can only process applications for signers associated to their own Corporation.

The application for certificates which are made directly to Firmaprofesional must include a document signed, either manually or digitally, by the legal representative of the Corporation, which authorises the issue of these certificates and indicates the name, surnames, ID number and position in the organization of each authorized person. The applicant may only request certificates for those persons who have been previously identified through the internal procedures within the last 5 years. In this way it will not be necessary for the signer to present themselves personally to Firmaprofesional.

In the case of an individual businessperson the applicant need only present the necessary documentation showing they are part of the Social Security system, such as a bank receipt with the corresponding payment.

c) **Processing**

Each Firmaprofesional Registration Authority will have a number of people accredited to act as an RA Operator in their dealings with Firmaprofesional. The RA Operators have been authorized by the RA to perform this function and have been previously trained in the operation of issuing certificates. Each RA Operator will have a Digital Certificate on their own QSCD, permitting them to manage user certificate requests.

The processing stages are as follows:

1. **Key generation**

The RA Operator validates the veracity and accuracy of the signer's details.

If necessary the RA Operator will organize for the signer the generation of the keys in an electronic signature creation device.

The RA Operator will verify that the signer is in possession of the private key (signature creation data) associated with the public key (signature verification data) included in the certification request.

2. Issuance of certificates

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

Firmaprofesional will verify the integrity of the request that has been generated by a duly authorized RA operator. After this validation they will proceed to issue the certificate.

In cases where Firmaprofesional has a guarantee that the device that generated the key pair is a QSCD, the certificate will be emitted with the corresponding OID.

3. Delivery

Once the certificate is generated and before the RA can deliver it to the applicant, the latter must:

- Appear before the RA in accordance with Article 13 of Law 59/2003, except in cases where their presence is not required for the collection.
- Formally accept delivery of the certificate and leave documentary evidence with the RA.

Finally, the RA will present the certificate to the signer, either handing them the portable QSCD, the authentication mechanisms and remote electronic signature operation or enabling the mechanisms for their download and later use.

In cases where the applicant acts on behalf of another natural person they must obtain the acceptance of the certificate by the signer before the certificate can be considered valid. In this case, the certificate will be issued with a grace period during which the certificate is not valid. After the grace period, if the applicant has the means to access the private key and has not obtained the formal acceptance of the certificate by the signer, the applicant must revoke the certificate immediately. Otherwise the applicant will be liable for all damages that may result from the use of the certificate, especially those concerning the protection of personal data of the signer.

By following these procedures, Firmaprofesional guarantees that no signer has the certificate before completing the process of presenting themselves, as required under Article 13 of Law 59/2003.

4.2. CERTIFICATE REVOCATION

As specified in the Certification Practice Statement (CPS).

4.3. RENEWAL OF CERTIFICATES

There exist two procedures:

- a) **Process of renewal in person:** The signer must contact their RA and proceed with the generation of a new certificate.
- b) **Process of renewal online:** If the RA has the service available and the signer has requested a renewal, the latter will receive a notification from the RA to begin the renewal process through the web page of Firmaprofesional. The period of validity of certificates renewed online will be determined by the conditions set out in Article 13.4 of Law 59/2003.

5. CERTIFICATE PROFILE

5.1. DISTINGUISHED NAME (DN)

DN Field	Name	Description
CN, Common Name	Name	<i>Name and Surnames of the signer</i>
E, E-mail (Opcional)	E-mail	<i>E-mail of the signer</i>
O, Organization	Organization	<i>Name of the subscriber (company or private or public entity) with which the signer has an association</i> <i>In case the subscriber is self employed, the commercial name of their establishment can be included, their CNAE (National Classification of Economic Activities) or IAE (Tax on Economic Activities)</i>
1.3.6.1.4.1.4710.1.3.2 ¹	Organization's TIN	<i>Tax Identification Number (TIN), VAT number or equivalent for Spanish companies (in Spanish, CIF, Código de Identificación Fiscal) corresponding to the person or entity which the signer is associated with.</i>
OrganizationIdentifier	Organization's TIN	<i>Tax Identification Number (TIN), VAT number or equivalent for Spanish companies (in Spanish, CIF, Código de Identificación Fiscal) corresponding to the person or entity which the signer is associated with, exactly as it appears in the official registers. Coded according to the European law ETSI EN 319 412-1 (Ej: VATES-B0085974Z)</i>
OU, Organization Unit	Organization unit	<i>Containing one of the following values:</i> <ul style="list-style-type: none"> • <i>The department to which the signer belongs</i> • <i>Type of association with the organization.</i>
T, Title	Title	<i>Position, title or role of the signer in the organization.</i>
ST, State	Geographical location	<i>Geographical area associated with the signer</i>
C, Country	Country	<i>Two digit country code, according to ISO 3166-1. "ES" by default.</i>
serialNumber	Serial number	<i>TIN for a natural person (in Spanish NIF) or Identity number or passport number of the signer².</i>
SN, surName	Surname	<i>Surnames of the signer exactly as they appear in the presented ID document</i>
GN, givenName	Given name	<i>Given name of the signer exactly as it appears as in the presented ID document</i>

¹ OID property of the company Safelayer Secure Communications SA, dedicated to contain a Tax Identification Number, VAT number or equivalent (CIF, Código de Identificación Fiscal, for Spanish companies; NIF, Número de Identificación Fiscal, for a natural person in Spain)

² In case the signer doesn't have an TIN for a natural person (in Spanish NIF) or ID number for foreigners (in Spanish NIE), a passport number must be provided in the format indicated in the corresponding section of the CPS.

5.2. COMMON CERTIFICATE EXTENSIONS

Extension	Note	Values
X509v3 Subject Alternative Name	-	<p><i>(Optional) RFC822:<signers' email></i></p> <p><i>directoryName:</i></p> <p>1.3.6.1.4.1.13177.0.1: Given name of the natural person exactly as it appears in the presented ID document.</p> <p>1.3.6.1.4.1.13177.0.2: First surname of the natural person exactly as it appears in the presented ID document</p> <p>1.3.6.1.4.1.13177.0.3: Second surname of the natural person exactly as it appears in the presented ID document (this field may be left empty)</p>
X509v3 Basic Constraints	Yes	<i>CA:FALSE</i>
X509v3 Key Usage	Yes	<p><i>Digital Signature</i></p> <p><i>Content Commitment</i></p> <p><i>Key Encipherment</i></p>
X509v3 Extended Key Usage	-	<p><i>TLS Web Client Authentication</i></p> <p><i>E-mail Protection</i></p>
X509v3 Subject Key Identifier	-	<i><id of the public key of the certificate, obtained from the hash of the certificate></i>
X509v3 Authority Key Identifier	-	<i><iid of the public key of the CA's certificate, obtained from the hash of the CA's certificate></i>
X509v3 CRL Distribution Points	-	<i><URI of the CRL></i>
X509v3 Authority Information Access	-	<p><i>Access Method: Id-ad-ocsp</i></p> <p><i>Access Location: <URI that gives access to the OCSP service></i></p> <p><i>Access Method: Id-ad-calssuers</i></p> <p><i>Access Location: <URI that gives access to the certificate of the issuing CA></i></p>
QcStatements	-	<p><i>Id-etsi-qcs-QcCompliance: 0.4.0.1862.1.1</i> <i>(indicating that the certificate qualified)</i></p> <p><i>Id-etsi-qcs-QcRetentionPeriod: 0.4.0.1862.1.3</i> <i>(with a value of 15 years)</i></p> <p><i>Id-etsi-qcs-QcPDS³: 0.4.0.1862.1.5</i> <i>(URI: https://www.firmaprofesional.com/cps/pds_en.pdf)</i></p> <p><i>Id-etsi-qcs-QcType: 0.4.0.1862.1.6.1</i> <i>(qct-esign, indicates that it is a certificate to create electronic signatures).</i></p>

³Mandatory in English. QcPDS can be included in other languages.

5.3. EXTENSIONS OF THE CERTIFICATES WITHOUT QSCD

Extension	Note	Values
X509v3 Certificate Policies	-	<p><OID of the certification policy corresponding to the certificate> 1.3.6.1.4.1.13177.10.1.2.2</p> <p><URI of the CPS></p> <p>User Notice: “Éste es un Certificado Corporativo de Persona Física cualificado para su uso sin DCCF. Dirección del prestador de Servicios de Confianza: Paseo de la Bonanova, 47. 08017 Barcelona”⁴</p> <p><OID of the European certification policy: 0.4.0.194112.1.0> (Corresponding to the policy for qualified EU certificates issued to natural persons “QCP-n”, without using a QSCD)</p>

5.4. EXTENSIONS OF THE CERTIFICATES WITH QSCD

Extension	Note	Values
X509v3 Certificate Policies	-	<p><OID of the certification policy corresponding to the certificate> 1.3.6.1.4.1.13177.10.1.2.1: QSCD portable 1.3.6.1.4.1.13177.10.1.2.3: QSCD centralized</p> <p><URI of the CPS></p> <p>User Notice: “Éste es un Certificado Corporativo de Persona Física cualificado para su uso conjuntamente con un DCCF. Dirección del prestador de Servicios de Confianza: Paseo de la Bonanova, 47. 08017 Barcelona”⁵</p> <p><OID of the European certification policy: 0.4.0.194112.1.2> (Corresponding to the policy for qualified EU certificates issued to natural persons “QCP-n-qscd”, using a QSCD)</p>
QcStatements	-	<p>Id-etsi-qcs-QcSSCD: 0.4.0.1862.1.4 (indicates that a private key is kept on a QSCD)</p>

⁴ “This is a Corporate Certificate for Natural Persons qualified for use without a QSCD. The address of the Trust Service Provider: Paseo de la Bonanova, 47. 08017 Barcelona”

⁵ “This is a qualified Corporate Certificate for Natural Persons to use in conjunction with a QSCD. The address of the Trust Service Provider: Paseo de la Bonanova, 47. 08017 Barcelona”