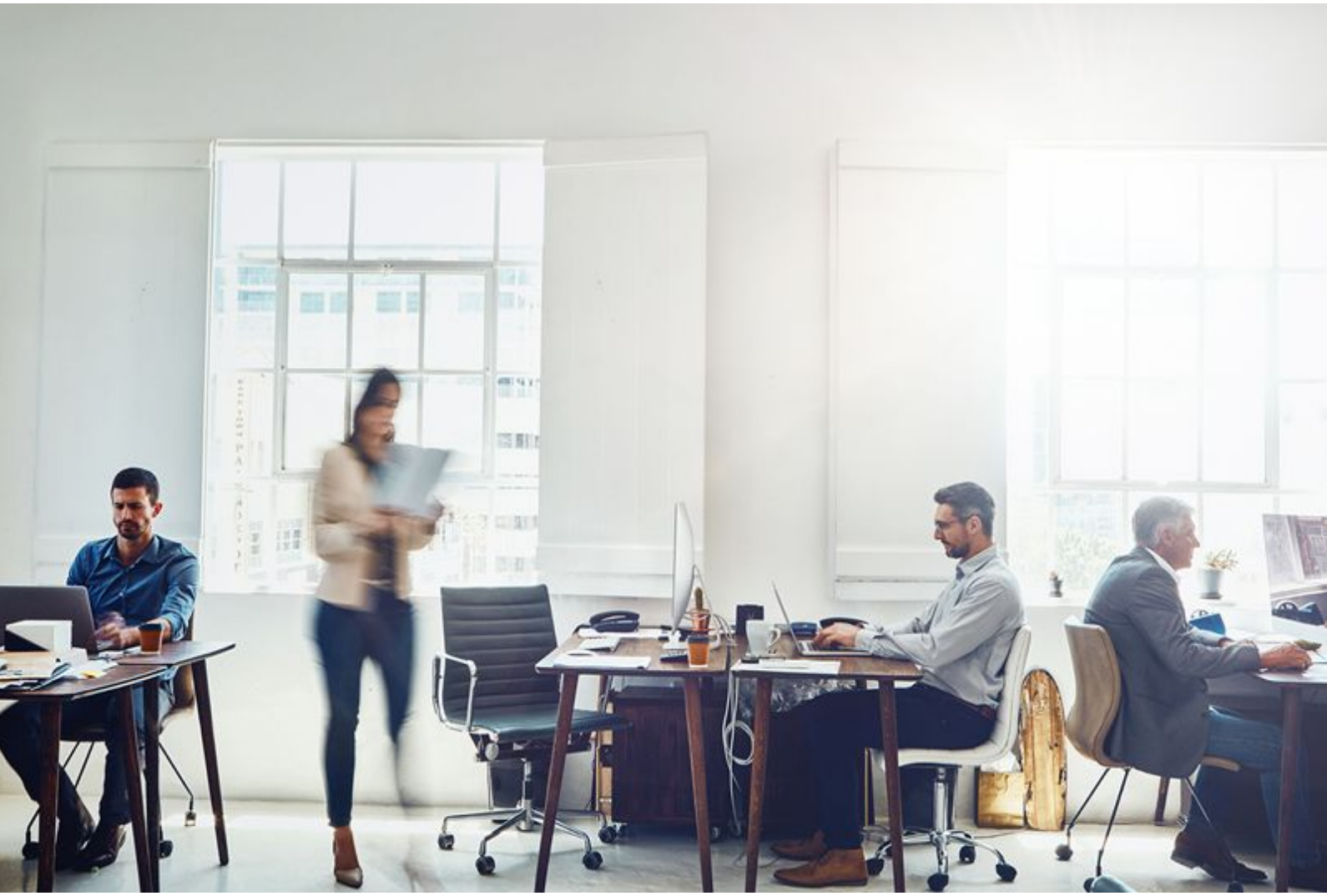
Certification Policy

Secure Service Certificates

Version: 190121

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
6.0	(in order to consult changes between previous versions, please send an email to info@firmaprofesional.com)	15/04/2014
190121	Addition of CA certificates. Segregation by TSA, VA and CA service certificates, and differentiation of certificates dedicated to qualified services. Removal of certificate Profile extensions in order to add within the document "Certificate Profiles of Firmaprofesional". Inclusion of causes for CA certificate revocation as requirement of CAB/forum. Template update	21/01/2019

Index

1. Introduction

1.1. General Description

Secure Service Certificates allow signing digital evidences as Certification Authority (CA). Their issuance and usage require maximum security guarantees.

These certificates will only be issued to entities of recognised prestige that have established a previous collaboration agreement with Firmaprofesional. These entities must have an HSM device certified FIPS 140-2 Level 3 for custody of the certificate private key.

Firmaprofesional may issue Qualified and Non Qualified Secure Service Certificates according to requirements established in Regulation EU 910/2014 of the European Parliament and of the Council of 23rd July 2014.

Within each group (qualified and non qualified), the different types of secure service certificates are included:

- CA Certificates
- Validation Certificates (VA)
- Time Stamp Certificates (TSA)

Specific conditions regarding these certificates are described in this document. This Certification Policy is subordinate to compliance with General Conditions defined within the Certification Practices Statement (CPS) of Firmaprofesional.

1.2. Identification of the Document

Name:	Certification Policy for Secure Service Certificates
Version:	190121
Description:	Certification Policy for Non Qualified Secure Service Certificates (CA, VA, TSA), and Qualified Secure Service Certificates (QCA, QVA, QTSA).
Date of issuance:	21/01/2019

OIDs	• CA: 1.3.6.1.4.1.13177.10.10.2 • VA: 1.3.6.1.4.1.13177.10.1.31.2 • TSA: 1.3.6.1.4.1.13177.10.1.4.2 • QCA: 1.3.6.1.4.1.13177.10.1.10.1 • QVA: 1.3.6.1.4.1.13177.10.1.31.1 • QTSA: 1.3.6.1.4.1.13177.10.1.4.1
Location	http://www.firmaprofesional.com/cps

2. Participating entities

2.1. Certification Authorities (CA)

Secure Service Certificates shall be issued by the following Certification Authorities:

- CA Certificates: issued by CA root of Firmaprofesional.
- TSA Certificates: issued by CA INFRAESTRUCTURA
- VA Certificates: issued by the same CA that issues the End-Entity certificates subject to validation.

Management of applications and issuances will be performed directly by Firmaprofesional.

Firmaprofesional will establish:

- The criteria to be complied with in order to request a certificate.
- The necessary mechanisms and procedures to perform both identification and authentication of the signatory, in compliance with the CPS.

2.2. Applicant

Certificates will only be issued to entities of recognised prestige that establish a previous collaboration agreement with Firmaprofesional.

2.3. Subscriber

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

2.4. Third parties trusting in certificates

Third parties trusting in certificates shall acknowledge their usage limitations

3. Certificate features

3.1. Certificate validity period

Profile	Qualified	Non Qualified
CA	At a minimum of 12 years	At a minimum of 12 years
VA	1 year	1 year
TSA	Certificate: 6 years Private key use: 3 years	Certificate and private key: 6 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.

CA and QCA certificates may be used for the following purposes:

- To guarantee the integrity of issued certificates
- To identify the signatory entity of the certificate

VA and QVA certificates may be used for the following purposes:

- To guarantee the integrity of the OCSP responses
- To identify the signatory entity

TSA and QTSA certificates may be used for the following purposes:

- To guarantee the integrity of the issued time stamps
- To identify the signatory entity

3.2.2. Non authorised use of certificates

Usage that contravenes any convention defined in this Policy and the Certification Practices Statement is not allowed.

CA and QCA certificates that do not belong to Firmaprofesional cannot issue Authentication Web Certificates (SSL) in any of their modalities, including Electronic Office. In order to avoid this, these certificates will be issued "Technically Constrain".

4. Operational procedures

4.1. Certificate issuance process

Issuance process for all secure service certificate modalities will be manually operated by the Technical Director of Firmaprofesional, as the authorised operator.

4.1.1. Application

Certificates will only be issued to entities of recognised prestige that establish a previous collaboration agreement with Firmaprofesional.

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

The Technical Director of Firmaprofesional will verify compliance with security requirements for the proposed infrastructure.

4.1.2. Application acceptance

Firmaprofesional will only accept applications that comply with requirements established for each type of certificate.

Common requirements to all secure service certificates:

- Document signed by hand or digitally by the Legal Representative of the corporation authorising the issuance of these certificates.
- In cases where the corporation is Firmaprofesional itself, approval from the Technical Director will be sufficient.

4.1.3. Application processing

Firmaprofesional will verify identity and operational capacity of the applicant entity.

If the information provided in the application is incorrect or insufficient, the RA will deny the application and shall contact the applicant to communicate the reasons. Otherwise, the legal instrument between the subscriber or the applicant and Firmaprofesional will be signed.

In addition to specifications regarding the issuance of digital certificates in the CPS:

- The issuance processing of these certificates will require direct supervision from the Technical Department of Firmaprofesional.
- The issuance processing of these certificates will be performed by hand following the maximum security guarantees.
- Physical access to TSP system components where security is critical for the trust services provision, will be limited to authorised persons.

4.1.3.1. VA, QVA, TSA and CA certificates

Generation of keys for signature of OCSP responses must be performed in a secure space, within cryptographic devices (HSM 140-2 Level 3) by appropriate personnel according to trust roles.

The cryptographic suite chosen for each type of certificate will be considered secure at the time of issuance for the duration of the certificate. Regulation ETSI TS 119 312 version in force at the time of the issuance or equivalent will be the reference for such consideration.

4.1.3.2. QCA / QTSA certificates

Additionally, application processing will be performed at least with a dual control and witnesses of Firmaprofesional, CA holder organisation and outside auditor. Also, all activity relating to generation of QCA certificate keys will be recorded in a affidavit.

For TSA and QTSA cases, the private key generated for a TSU may only be imported into other cryptographic modules for the purpose of providing High Availability of the service.

Technical Director of Firmaprofesional will manage online obtention of the certificate. Generated keys and certificate will remain secured within the HSM.

4.2. Certificate revocation

Due to the specific features of theses type of certificates, their revocation will require authorisation from the Technical Director or Innovation, Compliance and Technology Director of Firmaprofesional.

This procedure is applicable to all policies included in this document.

Specifically, Firmaprofesional will revoke a Subordinate CA certificate within a seven (7) days period under the following circumstances:

1. The subordinate CA requests the revocation in writing;
2. The subordinate CA notifies Firmaprofesional that the original application was not authorised and does not grant retroactive authorisation;
3. Firmaprofesional obtains proof that the private key of the subordinate CA corresponding to the public key in the certificate has been compromised or does not comply with key size or public key and quality parameters.
4. Firmaprofesional obtains proof that the certificate has been used fraudulently;
5. Firmaprofesional acknowledges that the certificate was not duly issued, or the Subordinate CA has not complied with this Certification Policy or the CPS;
6. Firmaprofesional determines that some information in the certificate in false or incorrect.
7. Firmaprofesional or the Subordinate CA cease operation for any reason and have not agreed with other CA the provision of support for the revocation of the certificate;

8. The right of Firmaprofesional or the subordinate CA to issue certificates under the requirements of this Policy has expired, revoked or finish, unless Firmaprofesional has achieved an agreement with other entity for this to maintain the CRL/OCSP Repository;

9. Revocation is required by the Certification Practices Statement of Firmaprofesional.

4.3. Certificate renewal

Renewal of all certificate modalities included in the policy will imply following the new certificate generation process. This issuance must be performed before the expiration of the previous certificate, applying all actions needed to avoid operations disruption. The new certificate will be issued according to requirements of this policy.

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
Certification Authority Certificate (CA)	1.3.6.1.4.1.13177.10.10.2
Validation Certificate (VA)	1.3.6.1.4.1.13177.10.1.31.2
Time Stamp Certificate (TSA)	1.3.6.1.4.1.13177.10.1.4.2
Qualified Certification Authority Certificate (QCA)	1.3.6.1.4.1.13177.10.1.10.1
Qualified Validation Certificate (QVA)	1.3.6.1.4.1.13177.10.1.31.1
Qualified Time Stamp Certificate (QTSA)	1.3.6.1.4.1.13177.10.1.4.1

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.

January 2019