firmaprofesional

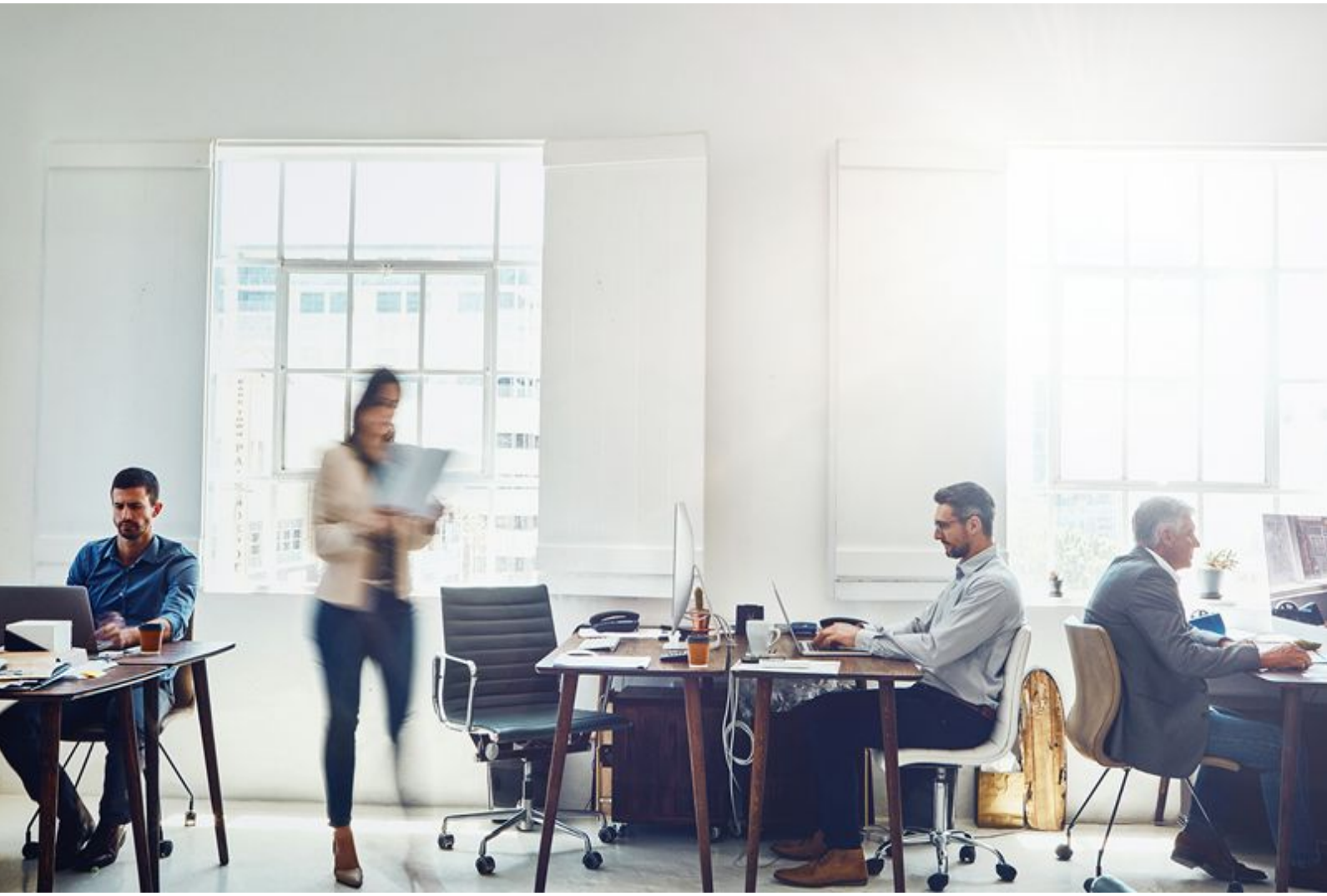
General Documentation

Certification Practices Statement (CPS)

Firmaprofesional, S.A.

Version: 190806

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
6.1	(to view changes between earlier versions, please send an email to info@firmaprofesional.com)	20/10/2014
151005	• "*1.3.2 Certification Authority (CA)*": o Limitation of CA Subordinates who may be issued certificates. o Limitation of CAs who may issue SSL, SSL EV certificates or equivalent. o Addition of identification, clarifications and incorporation of technical restrictions of the SHA2 certificates for the following CAs: ▪ Certification Authority Firmaprofesional CIF A62634068 ▪ CA Firmaprofesional – INFRAESTRUCTURA ▪ CA Firmaprofesional – CFEA ▪ CA Firmaprofesional – OTC ▪ SIGNE Certification Authority ▪ SEU Certification Authority ▪ Santander Digital Signature • "*1.4.3 Certificates for the Public Administration*": for functionality reasons the certificate is deleted from the Electronic Office and moved to the "Service Insurance Certificate" section. • "*2.1 Repositories*": the table is updated • "*5.8.2 Registration Authority*": also the RA is obliged to deliver all the documentation to Firmaprofesional. • "*6.1.5 Key size*": given the diversity of certification policies the definition of the period of validity for end entity certificates is open	05/10/2015
160229	• "*1.4.3 Certificates for the Public Administration*": clarifies the nature of the Electronic Office • "*1.3.2.2 Subordinate Public Certification Authorities*": the certificates of the "Electronic Office" are shown as issued by CA FIRMAPROFESIONAL - INFRAESTRUCTURA • The explicit reference to the version of the "Mozilla CA Certificate Inclusion Policy" and "Baseline Requirements	29/02/2016

	Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates" is deleted, referencing "the current version".	
171121	• "*5.3.5 Frequency and sequence of job rotation*" created section. • The entire document is inspected after the eIDAS review. • Safe Device is changed for Qualified Device. References to the law 11/2007 are eliminated. • References to Code Signing OID are eliminated.	21/11/2017
180704	• Inclusion of Corporate Certificates Representatives of an Entity without Legal Status. • Verification of adherence to Mozilla Root Store Policy, version 2.5. • Inclusion of course of action in case of vulnerability of cryptographic suite. • Elimination of the section Corporate certificates of restricted use and of the certificates of Infrastructure, of code signing and of electronic invoicing. • "*1.4.7. Request for a test certificates kit*": included section. • "*1.5.1 Notification of unauthorized uses, complaints or suggestions*": included section. • Inclusion of data of SHA256 Subordinate Certification Authority AC Firmaprofesional - AAPP. • Elimination of references to Advanced Electronic Signature. • (*Exclusively in English version*) Changed "Public Employee" by "Public Officer".	04/07/2018
181221	• "*1.4. Unauthorised use of the certificates*": removal of types of certificates. • Communication of revocation of CA Certificates for Banco Santander • Removal of the possibility for allowing certificates to be published in repositories. • Update to CA/Browser -Forum V.1.6.1 of October 2018 requirements in section 4.9	21/12/2018

	• Update of references to legislation regarding Personal Data Protection. Removal of the file registered in the Spanish Data Protection Agency (Agencia Española de Protección de Datos, or "AEPD") due to the deletion of AEPD Register. • Communication of revocation of CA CFEA and OTC certificates and new issuance of these same certificates with updated technical restrictions. • Communication of revocation of the CA INFRAESTRUCTURA certificate with hash SHA1. • Participating Entity Point of Verification in Person has been added. • Validity period of operator certificate is now between 1 and 5 years.	
190612	• One of the "INFRAESTRUCTURA" CAs has been revoked. Added revocation date. • Verification of adherence to Mozilla Root Store Policy, version 2.6.1. • Adding certificate revocation conditions for PSD2. • Addition of applicable PSD2 regulations. • "*4.4.2. Publication of the certificate*": Paragraph is added by issuance of certificates for PSD2.	12/06/2019
190806	• Restructuring of historical version points. • "*3.2.7. Identification of high risk certificates*": created section. • "*4.9.9. Requirements for checking revocation online*": added considerations for the use of the OCSP service. • "*5.4.7. Vulnerability assessments*": indicates the type of vulnerability analysis performed. • "*6.2.6. Private key transfer info or from a cryptographic module*": restructuring of the section. • "*9.14. Applicable regulations*": including adherence to the latest version of the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates".	06/08/2019

Index

1. Introduction

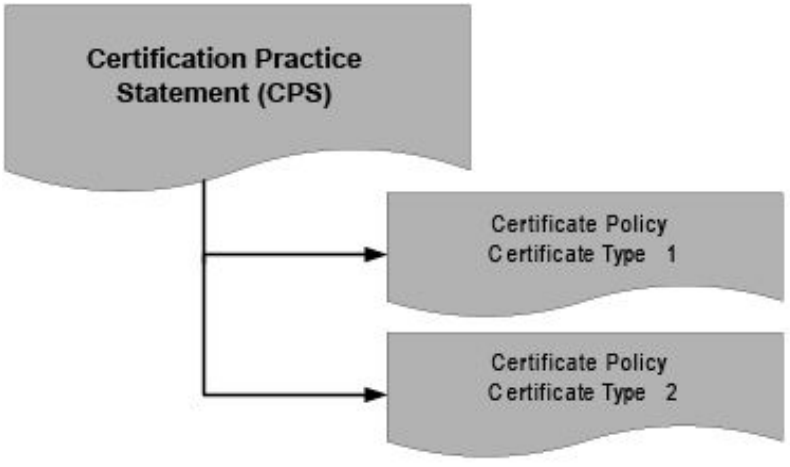
1.1. Presentation

Firmaprofesional S.A. began as a project involving several professional associations. It was declared a 'Sociedad Anónima' (Public Limited Company P.L.C.) in 2001 in order to act independently as a Certification Services Provider (CSP) that issues certificates recognised under the Law 59/2003, of 19 December, on electronic signatures.

The **Law 59/2003, of 19 December**, on electronic signatures requires that certification service providers keep custody of and permanently manage the electronic certificates which they have issued. Details of this management must be included in the so-called Certification Practice Statement where the conditions concerning the application, issuance, use, suspension and termination of the validity of the electronic certificates are specified. The purpose of the present document is to meet these requirements, established by law, so constituting the **Certification Practice Statement** of Firmaprofesional.

The structure of this document is based on the specifications of standard "RFC3647 - *Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework*", created by the working group PKIX of the IETF.

In addition to the terms and conditions set forth in this CPS, each type of certificate issued by Firmaprofesional is governed by the conditions contained in the **"PKI Disclosure Statement"** (**PDS**), as well as the requirements which may be found in the "**Certificate Policy**" **(CP**).



The certification service of Firmaprofesional conforms to Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, which repeals Directive 1999/93/CE.

The services of Firmaprofesional conform to the following ETSI standards:

- ETSI EN 319 401 (General Policy Requirements for Trust Service Providers)
- ETSI EN 319 411-1 (Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements)
- ETSI EN 319 411-2 (Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates)
- ETSI EN 319 412-1 (Certificate Profiles; Part 1: Overview and common data structures)
- ETSI EN 319 412-2 (Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons)
- ETSI EN 319 412-3 (Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons)
- ETSI EN 319 412-4 (Certificate Profiles; Part 4: Certificate profile for web site certificates)
- ETSI EN 319 412-5 (Certificate Profiles; Part 5: QCStatements)
- ETSI TS 119 495 (Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366)

1.2. Document Title

1.2.1. Identification

Name:	Certification Practice Statement (CPS)
Version:	190806
Description:	Certification Practice Statement of Firmaprofesional S.A..
Date of Issue:	08/06/2019
OID:	1.3.6.1.4.1.13177.10.0.190806
Web address:	http://www.firmaprofesional.com/cps

1.2.2. OIDs

Following the digital certification standards, Firmaprofesional uses Object Identifiers (OID) defined in the standard *ITU-T Rec. X.660 (2004) | ISO/IEC 9834-1:2005 "Procedures for the Operation of OSI Registration Authorities: General Procedures and ASN.1 Object Identifier tree top arcs"*.

Firmaprofesional registered in IANA as a private company with the OID number "**13177**".

(http://www.iana.org/assignments/enterprise-numbers).

OID's that begin with "1.3.6.1.4.1.13177" have the following meaning:

OID	Object Type	Description
10.0.190806	Certification Practice Statement (CPS)	Version of the document.

10.1.T.D	Certification Policies	T = Type of Certificate 1 = Corporate for professional associations 2 = Corporate for natural persons 3 = Web Server SSL and PSD2 4 = Secure Service TSA 5 = Corporate for legal persons 6 = Corporate for electronic invoicing 10 = Corporate Company Seal and PSD2 11 = Corporate for Legal Representatives 12 = Corporate for Voluntary Representative 13 = Corporate for Representatives of an Entity without Legal Status 20 = Electronic Office 21 = Organisation Seal 22 = Public Officer 23 = Public Officer with pseudonym 30 = Infrastructure Certificate 31 = Secure Service VA 40 = Personal Certificate D = Device / Security Level 1 = QSCD portable (High Level) or OV SSL or certificate for qualified services (TSA or VA secure service) 2 = Other devices (Intermediate Level) or certificates for not qualified services (TSA or VA secure service) 3 = QSCD centralised 10 = SSL EV and PSD2
10.10.N	Certificate Policy of Subordinate CA	1 = Qualified Subordinate CA 2 = Not Qualified Subordinate CA
20.0.1	Not Qualified Time Stamping Service Policy	
0.4.0.2023.1.1	Qualified Time Stamping Service Policy (according ETSI EN 319 421)	This OID does not have the prefix 1.3.6.1.4.1.13177, which identifies Firmaprofesional

1.3. Participating entities

1.3.1. Trust Service Provider (TSP)

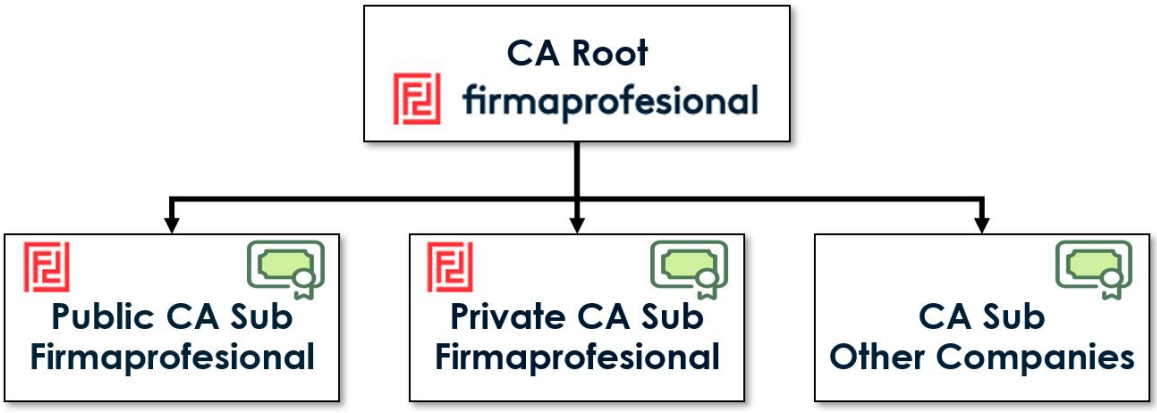
Firmaprofesional is a Trust Service Provider (TSP) that issues certificates pursuant to the Spanish Electronic Signatures Law.

Firmaprofesional is the issuing entity of certificates and is responsible for the life cycle and operation of the certificates during the life cycle. The functions of the authorisation, registration, issuance and revocation of the personal certificates of the end entity may be performed by other delegated entities, contracted by Firmaprofesional, who will act as intermediaries.

Firmaprofesional also provides electronic signature and time stamping validation services, which are governed by separate policies, not included in this document.

1.3.2. Certification Authority (CA)

The certification system of Firmaprofesional consists of various Certification Authorities (CA), which are arranged under a two level Certification Hierarchy, formed by a single Root CA and by various Subordinate CA's.



The subordinate CA's can be issued in Firmaprofesional's name or in the name of another TSP. In either case all CAs within the Firmaprofesional Certification Hierarchy must be operated technically by Firmaprofesional, within the infrastructure of Firmaprofesional.

Firmaprofesional is not authorised to issue a subordinate CA certificate for a TSP who operate

the PKI through their own means or with their own infrastructure. In this way Firmaprofesional can guarantee that the technical security of all the subordinate CAs is the same, regardless of the entity appearing as TSP.

If a TSP wishes to operate the PKI through their own means or with their own infrastructure, the status of Subordinate CA must be revoked and another CA created outside of the Firmaprofesional Hierarchy.

Firmaprofesional can operate other PKIs outside of the Firmaprofesional Hierarchy.

1.3.2.1. Root Certification Authority

The title Root Certification Authority (Root CA) will be given to the entity within the hierarchy which emits certificates to other certification authorities, and whose public key certifícate has been self-signed. Its function is to sign the certificate of the other CAs belonging to the Hierarchy of Certification.

There exist two versions of this certificate, both with the same key pairs and the same identification data, one generated with the algorithm SHA1 and the other using the SHA2 algorithm.

The identification details for the Root Certificate of Firmaprofesional are:

- ***CN: Certification Authority, Firmaprofesional CIF A62634068***
- *Hash SHA1: AEC5 FB3F C8E1 BFC4 E54F 0307 5A9A E800 B7F7 B6FA*
- *Valid from May 20, 2009 until December 31, 2030*
- *Key type: RSA 4096 bits – SHA1*

- ***CN: Certification Authority, Firmaprofesional CIF A62634068***
- *Hash SHA1: 0bbe c227 2249 cb39 aadb 355c 53e3 8cae 78ff b6fe*
- *Valid from September 23, 2014 until May 5, 2036*
- *Key type: RSA 4096 bits – SHA256*

Both Root CA certificates can be used together and interchangeably since all certificates

issued by Firmaprofesional are validated against both of these certificates.

Since December 2016 Firmaprofesional only issues end entity certificates in SHA256.

1.3.2.2. Public Subordinate Certification Authorities

The title Delegate or Subordinate Certification Authorities (SubCA) is given to entities within the certification hierarchy who emit end entity certificates and whose public key certificate has been digitally signed by the Root Certification Authority.

Public Subordinate Certification Authorities issue certificates that can be used publicly. These certificates are regulated by different agencies (such as the Ministry of Industry, Trade and Tourism -MINCOTUR-) and recognised by different platforms (such as Microsoft, Firefox, Chrome, Apple, Adobe, @Firma, PSIS and AEAT) and audited subject to different rules (such as Webtrust).

1.3.2.2.1. AC Firmaprofesional - CA1

The Subordinate Certification Authority "***AC Firmaprofesional - CA1***" issues digital certificates to Private Corporations, in accordance with the Law 59/2003 of 19 December on electronic signatures:

- ***CN = AC Firmaprofesional - CA1***
- *Hash SHA1: A366 C03C D7CB 1D13 90DE EBB9 67DF 588B 1A4E BFDE*
- *Valid from August 25, 2009 until June 16, 2030*
- *Key type: RSA 2048 bits – SHA1*

1.3.2.2.2. AC Firmaprofesional - AAPP

The Subordinate Certification Authority "***AC Firmaprofesional - AAPP***" issues digital certificates to Public Corporations, in accordance with the Law 40/2015 of 1 October of the Public Sector Legal System.

There exist two versions of this certificate, both with the same pair of key pair and the same identification data, one generated with the algorithm SHA1 and the other using the SHA2 algorithm.

- CN = AC Firmaprofesional – AAPP
- Hash SHA1: E678 37DC 4C75 EA77 458C 14C3 6B5C 0DA6 512C 6FC0
- Valid from July 7, 2010 until July 7, 2022
- Key Type: RSA 2048 bits – SHA-1

- CN = AC Firmaprofesional - AAPP
- Hash SHA1: 3E74 9302 FEB9 6904 AFEA 06FE 220A CBF4 08CF EDFA
- Valid from 25 de Octubre 2016 until 7 de Julio de 2022
- Key Type: RSA 2048 bits – SHA-2

1.3.2.2.3. AC Firmaprofesional - CUALIFICADOS

The Subordinate Certification Authority "***AC Firmaprofesional - CUALIFICADOS***" issues qualified digital certificates in accordance with the Law 59/2003 of 19 December on electronic signatures.

This CA is adapted to the requirements of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, which repeals the Directive 1999/93/CE (eIDAS)", and is issued with the SHA256 algorithm.

There are two versions of this certificate, both with the same key pair, identification data and end of term. They are distinguished by the fact that the most recent version has the field *Issuer* encoded in UTF8, in order to improve the compatibility:

- CN = AC Firmaprofesional - CUALIFICADOS
- Hash SHA1: 3486 ED23 6221 5545 9E9B 25FF 3F21 AD76 2798 7387
- Valid from September 18, 2014 until December 31, 2030
- Key type: RSA 2048 bits – SHA-256

- CN = AC Firmaprofesional - CUALIFICADOS
- Hash SHA1: 9F2B E8F3 E159 2F2F EC2C 6C88 A1C2 1579 286F 5CE8
- Valid from December 14, 2018 until December 31, 2030
- Key type: RSA 2048 bits - SHA-256

1.3.2.2.4. AC Firmaprofesional – INFRAESTRUCTURA

Subordinate Certification Authority "***AC Firmaprofesional – INFRAESTRUCTURA***" issues digital certificates for securing communications and services using cryptographic protocols compatible with PKI technology.

All the SSL and SSL EV certificates as well as Electronic Office certificates issued under the Firmaprofesional Certification Hierarchy must be issued by this CA. Therefore, no other CA of the Firmaprofesional Certification Hierarchy (whether public, private or other subordinate CSP) may issue SSL, SSL EV or Electronic Office certificates.

There exist two versions of this certificate, both with the same pair of key pair and the same identification data, one generated with the algorithm SHA1 and the other using the SHA2 algorithm. The latter is restricted technically via the extension *Extended Key Usage (EKU - extKeyUsage)* in accordance with the *Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates and Mozilla CA Certificate Inclusion Policy* which is in effect when this CPS comes into force.

- CN = AC Firmaprofesional – INFRAESTRUCTURA
- Hash SHA1: D52F 537F 62CE 24D0 6FB5 9B0A 02BF C4A8 F7C1 6B66
- Valid from June 18, 2013 until December 31, 2030
- Revocation date: April 13, 2018
- Key type: RSA 2048 bits – SHA1

- CN = AC Firmaprofesional – INFRAESTRUCTURA

- Hash SHA1: AC 1E 38 0A 14 DD D2 22 81 0D DB F4 CF 32 0F 1A FE 91 09 40
- Valid from July 29, 2015 until December 31, 2030
- Key type: RSA 2048 bits – SHA256
- Technical Restrictions (extendedKeyUsage):
  - Server authentication (1.3.6.1.5.5.7.3.1)
  - Client authentication (1.3.6.1.5.5.7.3.2)
  - Code signing (1.3.6.1.5.5.7.3.3)
  - Date stamping (1.3.6.1.5.5.7.3.8)
  - OCSP signing (1.3.6.1.5.5.7.3.9)

1.3.2.3. Private Subordinate Certification Authorities

Private Subordinate Certification Authorities issue certificates for private use between entities. They are not recognised in any platform nor are they regulated by any agency.

Firmaprofesional guarantees the same level of technical security to these certificates as to the public certificates, since they are operated from the same infrastructure and from the same facilities.

1.3.2.3.1. AC Firmaprofesional - CFEA

The Subordinate Certification Authority "**AC Firmaprofesional - CFEA**" issues not qualified digital certificates for electronic signature services.

There exist three versions of this certificate, both with the same pair of key pair and the same identification data, one generated with the algorithm SHA1 and two using the SHA2 algorithm. SHA2 versions are restricted technically via the extension *Extended Key Usage (EKU - extKeyUsage)* in accordance with the *Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates and Mozilla CA Certificate Inclusion Policy* which is in effect when this CPS comes into force.

- CN = AC Firmaprofesional - CFEA

- Hash SHA1: 6B66 7859 C1D8 C0F6 2F20 5B21 53D3 255C 7E16 CE0B
- Valid from February 20, 2013 until December 31, 2030
- Revocation date: November 16, 2018
- Key type: RSA 2048 bits – SHA1

- CN = AC Firmaprofesional - CFEA
- Hash SHA1: 3A 8F 3B B1 90 75 00 4A 29 CD 60 85 F3 49 2E 10 DA B1 B7 B2
- Valid from July 29, 2015 until December 31, 2030
- Revocation date: November 16, 2018
- Key type: RSA 2048 bits – SHA256
- Technical restrictions (extendedKeyUsage):
    - Client authentication (1.3.6.1.5.5.7.3.2)
    - Secure email (1.3.6.1.5.5.7.3.4)
    - OCSP signing (1.3.6.1.5.5.7.3.9)
    - Session start-up with smart card (1.3.6.1.4.1.311.20.2.2)

- CN = AC Firmaprofesional - CFEA
- Hash SHA1: A2F7 8768 6F62 5F66 0679 AAF1 C861 3CA3 841B 9087
- Valid from June 18, 2018 until December 31, 2030
- Key type: RSA 2048 bits - SHA256
- Technical restrictions (extendedKeyUsage):
    - Client authentication (1.3.6.1.5.5.7.3.2)
    - Session start-up with smart card (1.3.6.1.4.1.311.20.2.2)

- OCSP signing (1.3.6.1.5.5.7.3.9)
- Adobe Authentic Documents Trust (1.2.840.113583.1.1.5)

1.3.2.3.2. AC Firmaprofesional – OTC

The Subordinate Certification Authority "**AC Firmaprofesional - OTC**" (OTC: one-time certificate) issues not qualified digital certificates for services with electronic signatures. These certificates have a very short life span and are limited to the signing of a single document.

There exist three versions of this certificate, both with the same pair of key pair and the same identification data, one generated with the algorithm SHA1 and two using the SHA2 algorithm. SHA2 versions are restricted technically via the extension *Extended Key Usage (EKU - extKeyUsage)* in accordance with the *Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates and Mozilla CA Certificate Inclusion Policy* which is in effect when this CPS comes into force.

- CN = AC Firmaprofesional - OTC
- Hash SHA1: 1302 2ECD E763 0FB9 A14A 403E 74B0 FA3F A2A7 BCDA
- Valid from February 20, 2013 until December 31, 2030
- Revocation date: November 16, 2018
- Key type: RSA 2048 bits – SHA1

- CN = AC Firmaprofesional - OTC
- Hash SHA1: 6E13 B51C 6D54 0888 B8EC C236 79E9 1D99 AFF6 010D
- Valid from July 29, 2015 until December 31, 2030
- Revocation date: November 16, 2018
- Key type: RSA 2048 bits – SHA256
- Technical restrictions (extendedKeyUsage):
  - Client authentication (1.3.6.1.5.5.7.3.2)

- Secure email (1.3.6.1.5.5.7.3.4)
- OCSP signing (1.3.6.1.5.5.7.3.9)
- Session start-up with smart card (1.3.6.1.4.1.311.20.2.2)

- CN = AC Firmaprofesional - OTC
- Hash SHA1: 72DD 9D6D 7AE3 246C 6B9F 805F B2F6 216E 283C 4CE2
- Valid from June 18, 2018 until December 31, 2030
- Key type: RSA 2048 bits - SHA256
- Technical restrictions (extendedKeyUsage):
  - Client authentication (1.3.6.1.5.5.7.3.2)
  - Session start-up with smart card (1.3.6.1.4.1.311.20.2.2)
  - OCSP signing (1.3.6.1.5.5.7.3.9)
  - Adobe Authentic Documents Trust (1.2.840.113583.1.1.5)

1.3.2.4. Subordinate Certification Authorities of other TSPs

Under the Firmaprofesional Certification Hierarchy there resides several Subordinate CAs issued in the name of other entities. These other entities must act as Trust Service Providers and define their own Certification Practice Statement (CPS). Firmaprofesional guarantees the same level of technical safety to their certificates as to public certificates, since they are operated from the same infrastructure and the same facilities.

Currently the Hierarchy of Certification of Firmaprofesional incorporates the CAs of 3 other Trust Service Providers.

1.3.2.4.1. SIGNE Autoridad de Certificacion

SIGNE S.A. (CIF-A11029279) is a Spanish company whose main activity is the publication and printing of security documents for public and private companies.

There exist two versions of this certificate, both with the same key pair and the same

identification data, one generated with the algorithm SHA1 and the other using the SHA2 algorithm. The latter is restricted technically via the extension *Extended Key Usage (EKU - extKeyUsage)* in accordance with the *Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates and Mozilla CA Certificate Inclusion Policy* which is in effect when this CPS comes into force.

- CN = SIGNE Autoridad de Certificacion
- Hash SHA1: D730 47F2 CCE5 64EF B0BC 8568 93EA 19D7 7469 398C
- Valid from July 21, 2010 until July 21, 2022
- Key type: RSA 2048 bits – SHA1
- CPS: https://www.signe.es/signe-ac/dpc

- CN = SIGNE Autoridad de Certificacion
- Hash SHA1: E6B5 2B5D 52E5 CDE9 862A C1DE 668E C953 AD36 59BD
- Valid from July 29, 2015 until December 31, 2030
- Key type: RSA 2048 bits – SHA256
- Technical restrictions (extendedKeyUsage):
    - Client authentication (1.3.6.1.5.5.7.3.2)
    - Secure email (1.3.6.1.5.5.7.3.4)
    - OCSP signing (1.3.6.1.5.5.7.3.9)
    - Session start up with smart card (1.3.6.1.4.1.311.20.2.2)
- CPS: https://www.signe.es/signe-ac/dpc

1.3.2.4.2. SEU Autoridad de Certificacion

SEU (Servicios Electrónicos Universitarios) is a Colombian company focused on electronic administration in Colombian universities.

There exist two versions of this certificate, both with the same pair of key pair and the same identification data, one generated with the algorithm SHA1 and the other using the SHA2 algorithm. The latter is restricted technically via the extension *Extended Key Usage (EKU - extKeyUsage)* in accordance with the *Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates and Mozilla CA Certificate Inclusion Policy* which is in effect when this CPS comes into force.

Both certificates have been revoked due to the cessation of operations of this Trusted Services Provider.

- CN = SEU Autoridad de Certificacion
- Hash SHA1: 432C 2A08 ED3E 4ACB 87E8 4704 DCFD 9C3B D84D 18B7
- Valid from February 20, 2013 until December 31, 2030
- Revocation date: July 6, 2017
- Key type: RSA 2048 bits – SHA1
- CPS: http://www.seu.com.co/dpc

- CN = SEU Autoridad de Certificacion
- Hash SHA1: A9E5 5245 74A8 EC1F D316 1854 C913 4C47 97DE 7B09
- Valid from July 29, 2015 until December 31, 2030
- Revocation date: June 23, 2017
- Key type: RSA 2048 bits – SHA256
- Technical restrictions (extendedKeyUsage):
    - Client authentication (1.3.6.1.5.5.7.3.2)
    - Secure email (1.3.6.1.5.5.7.3.4)
    - OCSP signing (1.3.6.1.5.5.7.3.9)
    - Session start up with smart card (1.3.6.1.4.1.311.20.2.2)
- CPS: http://www.seu.com.co/dpc

1.3.2.4.3. Santander Digital Signature

Banco Santander offers its electronic certification services to universities by means of the University Smartcard ('Tarjeta Universitaria Inteligente', TUI).

There exist two versions of this certificate, both with the same pair of key pair and the same identification data, one generated with the algorithm SHA1 and the other using the SHA2 algorithm. The latter is restricted technically via the extension *Extended Key Usage (EKU - extKeyUsage)* in accordance with the *Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates and Mozilla CA Certificate Inclusion Policy* which is in effect when this CPS comes into force.

Both certificates have been revoked due to the cessation of operations of this Trusted Services Provider.

- CN = Santander Digital Signature
- Hash SHA1: CF4E 801B 2774 B820 6A62 6371 AE32 37B7 C1D4 3F4E
- Hash MD5: 1CD9 FA19 8BEE A19E 8658 7D90 58BE 3E88
- Valid from May 16, 2012 until December 31, 2030
- Revocation date: June 18, 2018
- Key type: RSA 2048 bits – SHA1
- CPS: http://www.tuisantander.com/cps

- CN=Santander Digital Signature
- Hash SHA1: B00C 0003 4B72 3F4D 9537 353C 8293 A945 514D AB2D
- Valid from July 29, 2015 until December 31, 2030
- Revocation date: June 18, 2018
- Key type: RSA 2048 bits – SHA256
- Technical restrictions (extendedKeyUsage):
    - Client authentication (1.3.6.1.5.5.7.3.2)
    - Secure email (1.3.6.1.5.5.7.3.4)

- OCSP signing (1.3.6.1.5.5.7.3.9)
- Session start up with smart card (1.3.6.1.4.1.311.20.2.2)

- CPS: http://www.tuisantander.com/cps

1.3.2.5. Expired Certification Authorities

1.3.2.5.1. Root Certification Authority

The original root certificate of Firmaprofesional expired on October 25, 2013. This certificate was replaced by a new Root Certificate with different keys.

- ***CN = Certification Authority, Firmaprofesional CIF A62634068***
- *Hash SHA1: A962 8F4B 98A9 1B48 35BA D2C1 4632 86BB 6664 6A8C*
- *Hash MD5: 1192 7940 3CB1 8340 E5AB 664A 6792 80DF*
- *Valid from October 25, 2001 until October 25, 2013*
- *RSA key length 2048 bits*

1.3.2.5.2. AC Firmaprofesional - CA1

The certificate of the Subordinate Certification Authority "*AC Firmaprofesional - CA1*" expired in 2013 and was also renewed.

In this case the same keys and name as before the renewal were retained. This certification model with shared keys is called "***Cross-Certification***[1]". As a result certificates issued to end-users could be validated equally well based on the CA hierarchy that expired in 2013 as with the CA hierarchy expiring in 2030.

The identification data of the Certificate of the Subordinate CA of Firmaprofesional which expired in 2013 are:

- CN = AC Firmaprofesional - CA1

[1]"Cross-certification" is a mechanism that allows the creation of multiple certification paths. In this case it permits the same certificate to be validated in either of two certification hierarchies which end in different CA roots. (See "RFC4949: Internet Security Glossary, Version 2": cross-certification).

- Hash SHA1: 037C F211 8F13 EAA6 121E B035 6F9B 601C 9295 338E
- Hash MD5: 35D8 35EC AF1C AF08 7DD5 8727 8AB2 0B19
- Valid from March 27, 2003 until March 26, 2013
- RSA key length 2048 bits

1.3.3. Registration Authority (RA)

A Registration Authority (RA) of Firmaprofesional is a body responsible for:

- Processing certificate applications.
- Identifying the applicant and ensuring they satisfy the necessary requirements for the certificate request.
- Validating the personal circumstances of the person to act as signatory for the certificate.
- Managing key generation and certificate issuance
- Delivering the certificate to the subscriber.

The following may act as an RA of Firmaprofesional:

- Any corporation that is a client of Firmaprofesional, to issue certificates in the name the corporation or to members of the corporation.
- Any trusted entity that arrives at an agreement with Firmaprofesional to act as an intermediary on behalf of Firmaprofesional.
- Firmaprofesional itself.

Firmaprofesional will contractually formalise the relationship between itself and each of the entities who act as an RA of Firmaprofesional.

The entity acting as an RA of Firmaprofesional may authorise one or more persons as the **RA Operator** to operate the certificate issuing computer system of Firmaprofesional on behalf of the RA.

In cases where the geographical location of the subscribers represents a logistical problem for subscriber identification and in the application for and delivery of certificates, the RA may delegate these functions to another trusted entity. This entity should have a special

relationship with the RA and a close relationship with the subscribers of the certificates in order to justify the delegation. The trusted entity must sign a collaboration agreement with the RA accepting the delegation of these functions. Firmaprofesional must be aware of and expressly authorise the agreement.

1.3.4. Point of Verification in Person (PVP)

Where the geographical location of the subscribers presents a logistical problem for identification, and for certificate request and delivery, the RA shall be able to delegate these functions to a trusted entity. In order to justify this delegation, the entity shall have an specific association with the RA and a close relationship with the certificate subscribers.

The trusted entity must sign a collaboration agreement with the RA in order to accept the delegations of these functions. Firmaprofesional must provide prior and express authorisation of the agreement model to be signed.

1.3.5. Applicant

The Applicant is a natural person who, in their own name or as the representative of a third party, makes a request to Firmaprofesional to issue a certificate.

The requirements to be met by an applicant will depend on the type of license requested and will be specified in the "Certification Policy" of each particular type of certificate.

1.3.6. Subscriber

The Subscriber is the natural or legal person who has contracted the trust services of Firmaprofesional. They will, therefore, be the owner of the certificate.

In general, the subscriber to a certificate of Firmaprofesional will be a professional association/public administration, public body or public legal agency/company. Their identity will appear on the certificate itself. In this case the subscriber may act as an RA, managing the issuance of certificates on behalf of the corporation or members of the corporation.

When Firmaprofesional sells the certificate directly to an individual, the subscriber and the signatory must be that same individual.

1.3.7. Signatory

The signatory is the natural person who possesses a signature creation device and who acts on their own behalf or, equally, as a representative of a professional association/public administration, agency or public legal entity/company, or the certificate subscriber.

The signatory has custody of the signature creation data associated with each of the electronic certificates.

1.3.8. Relying Party

The relying party is understood to be any person or organisation who voluntarily trusts in a certificate issued by Firmaprofesional.

The Qualified Certificates issued by Firmaprofesional are universal and are accepted by the majority of Spanish state agencies such as Ministries, Autonomous Communities, and Provincial or Local authorities. Firmaprofesional will try to establish agreements with the largest possible number of entities for the recognition of its Qualified Certificates.

The Root Certificates of Firmaprofesional are recognised by the leading software vendors such as Microsoft, Apple or Mozilla Foundation.

The obligations and responsibilities of Firmaprofesional with third parties who voluntarily trust certificates are limited to those contained in this CPS, in the Law 59/2003 on electronic signatures and in EU regulation 910/2014.

Certificate relying parties should be aware of the limitations on their use.

1.4. Unauthorised use of the certificates

Any use contrary to Spanish and European Union regulations, international agreements ratified by the Spanish state, good habits, morals and public order is not permitted. Furthermore any use other than that prescribed in this Certification Practice Statement and corresponding Certification Policy is not allowed.

Certificates have not been designed for, cannot be allocated to, neither is their use or resale authorised as control devices for dangerous situations or for uses requiring fail-safe operations, for the operation of nuclear facilities, air navigation or communication systems, weapons

control systems, or where failure could lead directly to death, personal injury or severe environmental damage.

End-user certificates can not be used to sign any type of public key certificates, neither can they sign certificate revocation lists.

Firmaprofesional does not store copies of the private keys of subscriber certificates. In case of loss or disablement of the private key or the device guarding the private key it is not possible to recover data encrypted with the corresponding public key for the Subscriber. A subscriber who decides to encrypt information does so, in all cases, under their own responsibility and consequently Firmaprofesional takes no responsibility for loss of data resulting from the loss of encryption keys. For this reason Firmaprofesional does not recommend the use of digital certificates for the encryption of information.

1.4.1. Notification of unauthorized uses, complaints or suggestions

In case of detecting an unauthorized use of the certificates or have a complaint or suggestion, they must be sent to Firmaprofesional by e-mail to the address soporte@firmaprofesional.com , indicating in the title whether it is an "Unauthorized Use", a "Complaint" or a "Suggestion" and attaching documents to prove the facts explained.

1.5. Policy Administration

1.5.1. Responsible Organisation

The Technical Department of Firmaprofesional is responsible for the administration of this CPS, the Certification Policies and of the PKI Disclosure Statements (PDS).

1.5.2. Contact person

Responsible Organisation:	Firmaprofesional, S.A.
Contact Person:	Compliance Officer of Firmaprofesional
E-mail:	compliance@firmaprofesional.com
Telephone:	+34 93 477 42 45

Address:	Firmaprofesional, S.A. Edificio ESADECREAPOLIS Avenida Torre Blanca, 57. Sant Cugat del Valles 08173 (Barcelona)

1.5.3. Frequency of Review

The CPS, CPs and PDSs will be reviewed and, if appropriate, updated annually.

1.5.4. Approval Procedure

The publication of the revisions of this CPS, the Certification Policies and PDS of each type of certificate must be approved by the Director General of Firmaprofesional, after checking for compliance with the requirements expressed in it.

1.6. Definitions and acronyms

1.6.1. Definitions

- **Certification Service Provider:** natural or legal person who issues electronic certificates or provides other services related to electronic signatures.
- **Trust Service Provider:** natural or legal person that provides one or more trusted services, either as qualified or non-qualified provider.
- **Electronic Certificate:** a document signed electronically by a Certification Service Provider which links certain data for signature verification to a signatory and confirms their identity
- **Recognised Certificate:** a certificate issued by a Certification Service Provider which meets the requirements set out by the law concerning verification of the identity and other circumstances of the applicants as well as the reliability and guarantees of the trust services which they provide, pursuant to chapter II of Title II of Law 59/2003 of 19 December on electronic signatures.

- **Qualified Certificate:** a certificate issued by a Qualified Provider of Secure Services and that meets the requirements set out in Annex I of Regulation (EU) 910/2014.
- **Public Key and Private Key:** asymmetric cryptography on which the PKI is based. It uses a key pair such that what is encrypted by one of them can only be decrypted by the other and vice versa. One of these keys is called the public key and it is included in the electronic certificate, while the other is called the private key and is known only to the certificate holder.
- **Conformity Assessment Body:** bodies accredited by member states to be able to issue compliance assessment reports as required by eIDAS.
- **Signature Creation Data (Private Key):** unique data, such as codes or private cryptographic keys, that the signatory uses to create the electronic signature.
- **Signature Verification Data (Public Key)**: data, such as codes or public cryptographic keys, which are used to verify the electronic signature.
- **Secure Signature Creation Device (SSCD):** device used to apply the data for the signature creation in compliance with the requirements set out in Article 24.3 of the Law 59/2003, of 19 December, on electronic signatures.
- **Qualified Signature Creation Device (QSCD)/or Seal Creation:** a device for the creation of electronic signatures that satisfies the requirements listed in Annex II of 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 in the internal market.
- **Electronic signature:** is the data set, in electronic form, attached to others or associated with them, which can be used as a means of personal identification.
- **Advanced Electronic Signature:** is the electronic signature which allows the personal identity of the signatory to be established with respect to the signed data and verifies its integrity by being exclusively linked to both the signatory and the data to which it refers, and by having being created in a manner that maintains it under their sole control.
- **Qualified Electronic Signature:** an advanced electronic signature based on a qualified certificate and generated by a Secure Signature Creation Device.
- **Hash function:** an operation performed on a data set of any size, in such a way that, regardless of the original size, the result is another data set of fixed size, and which has

the property of being associated unambiguously with the initial data.

- **Certificate Revocation List (CRL):** list containing the links for revoked or suspended certificates.
- **Hardware Security Module (HSM):** a hardware module used to perform cryptographic functions and to store keys in safe mode.
- **Electronic Time Stamp:** a special type of electronic signature issued by a trusted third party which allows the integrity of a document at a specific date and time to be guaranteed.
- **Qualified Electronic Time Stamp:** an electronic time stamp which satisfies the requirements set out in Article 42 of Regulation (EU) 910/2014.
- **Time Stamping Authority (TSA):** a trusted entity that issues time stamps.
- **Validation Authority (VA):** a trusted entity that provides information about the validity of digital certificates and electronic signatures.

1.6.2. Acronyms

CA:	Certification Authority
CAB:	Conformity Assessment Body
CP:	Certificate Policy
CPS:	Certification Practice Statement
CRL:	Certificate Revocation List
HSM:	Hardware Security Module
LDAP:	Lightweight Directory Access Protocol
OCSP:	Online Certificate Status Protocol
OID:	Object Identifier
PDS	PKI Disclosure Statement
PKI:	Public Key Infrastructure
PSC:	Certification Service Provider
RA:	Registration Authority
Sub CA:	Subordinate Certification Authority
TSA:	Time Stamping Authority
VA	Validation Authority

Standards and Organisations of Standardisation

CEN:	European Committee for Standardisation (Comité Européen de Normalisation)
CWA:	CEN Workshop Agreement
ETSI:	European Telecommunications Standard Institute
FIPS:	Federal Information Processing Standard
IETF:	Internet Engineering Task Force
PKIX:	Working group of the IETF dealing with PKI
PKCS:	Public Key Cryptography Standards
RFC:	Request For Comments

2. REPOSITORIES AND PUBLICATION OF INFORMATION

2.1. Repositories

Access	Description	URL
Public	CPS, Certification Policies and PDS	http://www.firmaprofesional.com/cps
Public	Root CA	http://crl.firmaprofesional.com/caroot.crt
Public	CRL of Root CA	http://crl.firmaprofesional.com/fproot.crl
Public	Subordinate CA CA1	http://crl.firmaprofesional.com/ca1.crt
Public	CRL of Subordinate CA CA1	http://crl.firmaprofesional.com/firmaprofesional1.crl
Public	Subordinate CA AAPP	http://crl.firmaprofesional.com/fpaapp.crt
Public	CRL of Subordinate CA AAPP	http://crl.firmaprofesional.com/fpaapp.crl
Public	Subordinate CA CUALIFICADOS	http://crl.firmaprofesional.com/cualificados.crt
Public	CRL of Sub CA CUALIFICADOS	http://crl.firmaprofesional.com/cualificados.crl
Public	Sub CA INFRAESTRUCTURA	http://crl.firmaprofesional.com/infraestructura.crt
Public	CRL of Sub CA INFRAESTRUCTURA	http://crl.firmaprofesional.com/infraestructura.crl
Public	Subordinate CA CFEA	http://crl.firmaprofesional.com/cfea.crt
Public	CRL of Sub CA CFEA	http://crl.firmaprofesional.com/cfea.crl
Public	Subordinate CA CFEA	http://crl.firmaprofesional.com/otc.crt
Public	CRL of Sub CA CFEA	http://crl.firmaprofesional.com/otc.crl
Public	Revocation Service	http://www.firmaprofesional.com
Restricted	Time Stamping Service (TSA)	http://servicios.firmaprofesional.com/tsa
Restricted	Validation Service (OCSP)	http://servicios.firmaprofesional.com/ocsp
Public	Validation Service (OCSP)	http://ocsp.firmaprofesional.com

Firmaprofesional repositories are referenced by URL. All entities that may be affected will be notified of any changes to the URLs .

The IP addresses corresponding to each URL may not be unique and may be dynamic, they

can be modified without previous notice.

2.2. Publication of information

2.2.1. Certification Policies and Practices

Both the current CPS, the Certification Policies and PKI Disclosure Statements for each type of certificate are available electronically on the Firmaprofesional's website.

Firmaprofesional keeps previously published versions as long as valid certificates exist which have been issued in accordance with these earlier versions.

Any other previous versions will be unavailable for online consultation, but may be requested by interested parties using Firmaprofesional's contact address.

2.2.2. Terms and Conditions

The contractual relationship between Firmaprofesional and the subscribers is based on the signing of a Contract to Provide Trust Services and the acceptance of the Certification Practice Statement, PDS and CP published on Firmaprofesional's website http://www.firmaprofesional.com/cps

2.2.3. Dissemination of certificates

The signatory (or, if they are not the same person, the subscriber to the certificate) will be responsible for delivering their certificate to any third parties wishing to authenticate a user or verify the validity of a signature. The delivery will usually be automatic, attaching the certificate to any electronically signed document.

2.3. Frequency of publication

The Root CA will issue an Authority Revocation List (ARL) at least every six months or, in extraordinary circumstances, with the revocation of a Certificate of Authority.

Each Subordinate CA will issue a Certificate Revocation List (CRL) daily, or in extraordinary circumstances, each time a certificate is suspended or revoked.

Firmaprofesional will immediately publish any changes to their certification policies and practices.

2.4. Access controls on repositories

The CPS, Certification Policy, PDS (PKI Disclosure Statement), CA certificates and Certificate Revocation Lists (CRL) will be published in repositories accessible to the public and without any access control.

The issued certificates are published in public repositories.

Following the OCSP, validation services will be free and with public access.

Following the TSP, Timestamping Services will have restricted access and incur a charge.

3. IDENTIFICATION AND AUTHENTICATION

3.1. Name Registration

3.1.1. Types of names

All certificates require a Distinguished Name (DN) in accordance with the X.500 standard. Further, all the names of qualified certificates are consistent with the provisions of section 7.1. Certificate profile.

3.1.2. Need for the names to be meaningful

The fields of the DN related to Full Name correspond to the legally registered data of the signatory, expressed exactly in the format shown on their National Identity Card, Residence Card, passport or other means recognised in law.

In the case that the information recorded in the DN are fictitious or explicitly indicate their invalidity (eg. "TEST" or "INVALID") the certificate will be considered without legal validity, and valid only to carry out technical tests for interoperability.

3.1.3. Use of pseudonyms

In general, the certificates do not allow the use of a pseudonym of the signatory, except and only with certificates of the type "public officer with pseudonym".

3.1.4. Rules for interpreting various name forms

In all cases Firmaprofesional follows the rules set out in the reference standard X.500 in ISO/IEC 9594.

3.1.5. Uniqueness of names

The distinguished name (DN) of the issued certificates will be unique for each subscriber or signatory. Whenever there is a problem with the duplication of names the CIF or NIF will be used to distinguish between the two.

3.1.6. Recognition, authentication and the role of trademarks

The CA accepts no liabilities from the issue of certificates with respect to the use by subscribers of a trademark. Firmaprofesional does not deliberately allow the use of a name whose right of use is not owned by the subscriber. However, the CA is not obliged to seek evidence of ownership of trademarks prior to issuing certificates.

3.2. Initial Identity Validation

3.2.1. Method to prove possession of private key

When a certificate is issued on a hardware device the private key is created immediately before the generation of the certificate by a process that guarantees its confidentiality and relation to the applicant's identity.

Each RA is responsible for ensuring the delivery or access to the applicant's device in a secure manner.

In other cases, the method of proof of possession of the private key by the subscriber will be the delivery of PKCS#10 or an equivalent cryptographic test or another method approved by

Firmaprofesional.

3.2.2. Authentication of the identity of a legal person

The Registration Authority must verify the following information in order to authenticate the identity of the organisation:

- The data concerning the business name or corporate name of the organisation.
- The data relating to the constitution and legal status of the subscriber.
- The data concerning the extent and validity of the powers of representation of the applicant.
- The data concerning the tax identification code of the organisation or equivalent code used in the country to whose legislation the subscriber is subject.

Firmaprofesional reserves the right not to issue the certificate if it considers that the documentation provided is not sufficient or adequate for verifying the above data.

3.2.3. Authentication of the identity of a natural person

The RA will verify the identity of the natural person identified in the certificate. To do this, the individual must appear in person and present their national identity card, residence card, passport or other legally recognised means of identification.

In cases where the Subscriber requests the modification of personal identification data from that shown in the presented identity document they must present the appropriate certificate from the Civil Registry which demonstrates the variation.

The RA will verify, either by the examination of sufficient original documentation, or with their own sources of information, the remaining data and attributes to be included in the certificate (distinguished name of the certificate), and must keep any documentation supporting the validity of data that cannot be checked through their own data sources.

The provisions set out in the preceding paragraphs will not be enforceable for certificates issued after the entry into force of Law 59/2003, of 19 December, on electronic signatures, in the following cases:

a. When the identity or other permanent circumstances of applicants for certificates are already on record with the RA due to a pre-existing relationship, which, for the

identification of the person concerned, the criteria mentioned in the first paragraph have been used and the time period that has passed since the identification is less than five years.

b. When applying for a certificate and another certificate is used where this previous certificate was issued after identifying the signatory in the manner prescribed in the first paragraph and the RA is satisfied that the period of time since the identification is less than five years.

3.2.4. Authentication of the identity of the RA and RA operators

For the creation of a new RA, the following actions will be performed:

- Firmaprofesional will verify the existence of the entity through its own sources of information.
- An authorised representative of the organisation must sign a contract with Firmaprofesional, which details the assignment of duties and responsibilities of each agent.

In addition, with respect to the RA operators, the RA will be required to fulfill the following conditions:

- To verify and validate the identity of the new RA operators. The RA must send Firmaprofesional the documentation corresponding to the new operator as well as their authorisation to act as an RA operator.
- To ensure that the RA operators have received sufficient training for the performance of their duties, they must have attended at least one operator training session.
- To ensure that communication between the RA and Firmaprofesional is conducted securely through the use of the operator's digital certificates.

3.2.5. Domain validation

To ensure that a requesting entity has control over the domain (URL) which it requests to include in certificate two types of checks must be performed:

- Organisational: the ownership of the domain name will be requested, certified by a legal representative of the organisation, as well as the name of the legal person to

whom the certificate is issued and, where applicable, the registration number, as recorded in the official records.

- Technical: The following WHOIS authentication services will be consulted:
    - For domains "*.es": https://www.nic.es/sgnd/dominio/publicInformacionDominios.action
    - For all other domains: http://www.iana.org/domains/root/db/ which is the WHOIS server authorised to seek information about the domain, depending on the top-level domain (TLD), that is, depending on whether the domain ends in .com, .org, .net, ...

3.2.6. Validation of email

In general, the signatories are persons linked to the Registration Authority (for example, members of professional associations, etc.). In these cases it is not the signatory who requests a specific email address to be included in the certificate, rather the RA itself which, consulting their databases, obtains the address.

In cases where the signatory has no connection with the RA, verification of the email address is carried out by challenge and response to the requested address.

3.2.7. Identification of high risk certificates

Firmaprofesional has methods to identify high-risk certificates through the use of blacklists, which require additional checks.

3.3. Identification and authentication for certificate renewal

3.3.1. Online renewal of certificates

The signatory can be identified and authenticated during the online renewal process by means of a qualified certificate provided they satisfy the following:

- The RA has authorised the renewal.
- The certificate to be renewed has not expired.
- In the case of Qualified Certificates, less than 5 years have elapsed since the last

appearance and identification before the RA[2].

Specific requirements may differ depending on the type of certificate requested and they will be set out in the corresponding "Certification Policy".

3.3.2. Renewal of certificates in person

The identification process will be carried out in the same way as when issuing a new certificate.

3.4. Identification and authentication for the revocation of certificates

The identification of the signatories in the process of certificate revocation may be performed by:

a. The signatory themself: identifying and authenticating themself using the Revocation Code provided on Firmaprofesional's website.

b. Any RA of Firmaprofesional: who will identify the signatory of a revocation request using whatever means they consider necessary.

c. In case of revocation of certificates for PSD2, whether web authentication or electronic seal, the revocation request can be made by the Bank of Spain or the Competent National Authority (ANC), by email to soporte@firmaprofesional.com containing a PDF sealed with a qualified certificate of electronic seal in the name of the ANC. The PDF must contain the data of the certificate to be revoked: at least the DN of the subject and the serial number of the certificate.

Each Certification Policy shall describe the applicable revocation process for certificates issued under its terms.

[2]In accordance of with Article 13, point 4b) of the law 59/2003, December 19, on electronic signatures

4. CERTIFICATE LIFE CYCLE OPERATIONAL REQUIREMENTS

4.1. Certificate applications

4.1.1. Who can apply for a certificate?

The requirements to be met by an applicant will depend on the type of license requested and will be set out in the "Certification Policy" of each specific type of certificate.

4.1.2. Certificate application processes

The applicant should contact Firmaprofesional directly or an Intermediary of Firmaprofesional that will act as an RA for the management of the certificate request.

The RA will provide the applicant with the following information:

- The documentation that is required in order to process the request and to verify the signatory's identity.
- Availability to perform the registration process.
- Information about the process of issuing and revocation, about safekeeping of the private key, as well as the responsibilities and conditions on the use of the certificate and the device.
- How to access and consult this document and the certification policies.

The documentation required for requesting each certificate type is specified in the Certification Policies (CP).

If the applicant is a corporation that acts as an RA of Firmaprofesional, the Corporation may directly manage the applications by securely accessing the computer system of Firmaprofesional and generating the appropriate certificates for the Corporation itself or for its members.

4.2. Processing of certificate applications

4.2.1. Performing identification and authentication functions

It is the responsibility of the RA to identify and authenticate the signatory. This process should be performed prior to issuing the certificate.

4.2.2. Approval or rejection of certificate applications

Once a certificate has been requested the RA will verify the information provided by the applicant, including validation of the signatory's identity.

If the information is not correct, the RA will reject the request and contact the applicant to inform them of the reason. If it is correct, the RA will proceed to the signing of a legally binding instrument between the subscriber and/or the applicant and Firmaprofesional.

They will then issue the certificate.

4.3. Issue of certificates

4.3.1. CA Actions during the issue of certificates

To issue certificates the following actions will be performed:

- A key pair will be generated in a secure manner, guaranteeing exclusive access for the signatory to the signature generation data.
- If necessary, the RA will deliver to the signatory the necessary mechanisms to allow the use of signature generation data (for example, physical delivery of the QSCD, activation codes, etc ...)
- If necessary, the signatory will deliver their public key to the RA.
- The RA will once again verify the contents of the certificate request against the provided documentation. If the verification is correct, the RA will validate the request.
- The RA will send the CA, via a secure channel, the public key of the signatory as well

as the verified data.

- The CA will verify the origin and integrity of the data sent by the RA.
- If all is correct, the CA will issue the certificate in a procedure that will use protection against forgery and maintain the confidentiality of the exchanged data .
- During the generation of the certificates, the CA will be responsible for adding the remaining information necessary to comply with the established technical and legal requirements.
- In cases where Firmaprofesional has assurances that the device which generated the key pair is a QSCD, the certificate will be issued with the corresponding OID.
- The generated certificate will be sent to the RA, which will then make it available to the signatory.

4.3.2. Notification to the Subscriber by the CA of the certificate's issue

The CA will notify the subscriber and/or signatory that the certificate has been issued and, if necessary, the download method.

4.4. Certificate Acceptance

4.4.1. How the certificate is accepted

The certificate will be accepted as soon as the legally binding instrument between the subscriber and Firmaprofesional has been signed and the certificate has been delivered, whether it be physically or electronically.

As proof of the acceptance the signatory must sign an acceptance form. The certificate is valid from the date on which this acceptance form is signed.

If the acceptance form is in electronic format the signatory must sign it using an advanced or qualified electronic signature.

4.4.2. Publication of the certificate

Once the certificate is generated and accepted by the subscriber or signatory, it may be

published in whichever certificate repositories are deemed necessary.

In case of issuance of PSD2 certificates, if Firmaprofesional has been notified about the email address of the ANC identified in the new issuance certificate, Firmaprofesional will send to this email address the information of the contents of the certificate including the serial number of the certificate in hexadecimal format, the subject the distinguished name of the subject, the distinguished name of the issuer, the period of validity of the certificate, as well as the contact information and instructions for revocation requests and a copy of the certificate file.

4.5. Use of the keys and certificate

4.5.1. Use of the private key and certificate by the subscriber

The certificates may be used in accordance with the stipulations of this CPS, the Certification Policy and the PKI Disclosure Statement.

The Key Usage extension may be used to establish the technical limits on the uses of the private key of the corresponding certificate. The application of these limits will depend primarily on the correct implementation by third-party computer applications, consequently its regulation is outside the scope of this document.

4.5.2. Use of the public key and certificate by relying parties

Relying parties may use certificates for the purposes agreed by this CPS and the corresponding Certification Policy.

It is the responsibility of relying parties to verify the certificate status using the services offered specifically for this purpose by Firmaprofesional and specified in the present document.

4.6. Certificate renewal without change of keys

This is not an option.

4.7. Certificate renewal with change of keys

There are two possibilities for the renewal of certificates:

a. In-person renewal process, which is carried out in the same way as when a new certificate is issued.

b. Online renewal process, which is detailed below.

4.7.1. Circumstances for online renewal

The online renewal of a certificate can only be carried out if the following conditions are met:

- The RA provides an online renewal service.
- The certificate has not expired.
- In the case of qualified certificates, less than 5 years have elapsed since the last presentation and identification before the RA[3].

4.7.2. Who can request the online renewal of a certificate

Any signatory may request the online renewal of their certificate provided they satisfy the circumstances described in the previous point.

4.7.3. Request for online renewal

A signatory may contact the RA that issued their certificate and request its renewal. The RA will then provide the signatory with information on how to formalise the request.

4.7.4. Processing online renewal requests

The following steps will be performed:

- The RA will receive a notification that a certificate is about to expire. The RA may then authorise immediate renewal.
- An email will be sent notifying the signatory that they can renew their certificate.
- The signatory will connect to the Firmaprofesional's webpage and, using their certificate, sign the renewal of the certificate.

[3]According to Article 13, point 4b) of the law 59/2003, December 19, on electronic signatures

- A new key pair will be generated.
- The public key will be sent to the CA via a secure channel, using the PKCS10 format or equivalent.
- The certificate will be generated immediately, using a procedure that protects against falsification and maintains the confidentiality of the exchanged data.
- The generated certificate will be delivered to the subscriber.

4.7.5. Notification of the issue of a renewed certificate

To formally finalise the process the CA will notify the subscriber and the signatory that the certificate has been renewed.

4.7.6. Form of acceptance of a renewed certificate

The certificate will be accepted upon the electronic signing of the renovation.

4.7.7. Publication of a renewed certificate

Once the certificate has been renewed, the new certificate may be published in whichever certificate repositories are deemed necessary, replacing the previous certificate, always on the condition that the signatory does not object to this publication.

4.8. Modification of certificates

If it is necessary to change any data, the RA should revoke the old certificate and issue a new one.

4.9. Revocation and suspension of certificates

The revocation of a certificate makes it invalid, this is irreversible.

The suspension[4] of a certificate makes it temporarily invalid, this is reversible.

Revocations and suspensions take effect from the moment they are published in the CRL.

4.9.1. Grounds for revocation

A certificate may be revoked for the following reasons:

a. Circumstances affecting the information contained in the certificate:

- Change of any of the data contained in the certificate.
- Discovery that any of the data contained in the application for the certificate is incorrect.
- In the case of Corporate certificates of a professional association, the signatory's loss of that body of membership.
- Loss or change of association of the signatory with the Corporation.
- The role of the payment service provider included in the PSD2 certificate has been revoked.

b. Circumstances affecting the security of the private key or the certificate:

- If the private key, infrastructure or systems of the CA have been compromised, whenever this affects the reliability of certificates issued subsequent to the incident.
- Infringement, by the CA or the RA, of the requirements set out in the procedures for the management of certificates, as established in the CPS.
- If the security of the key or of the subscriber's certificate is compromised or suspected of having been compromised.
- Unauthorised access or use, by a third party, of the private key of the subscriber.
- Irregular use of the certificate by the subscriber or signatory

c. Circumstances affecting the security of the cryptographic device:

[4]The suspended certificates appear in the CRL with the cause of revocation "Certificate Hold (6)" (RFC 5280). In some applications, after consulting the CRL, the Microsoft Windows operating system will translate the cause as "Possession of certificate (6)", which may induce a user error.

- If the security of the cryptographic device has been compromised, or is suspected of being compromised.
- If the cryptographic device is lost or no longer functional due to damage.
- Unauthorised access, by a third party, to the activation data of the subscriber.

d. Circumstances relating to the subscriber or signatory:

- Failure on the part of the subscriber or signatory to adhere to the usage rules of the certificate set out in the present CPS or the legally binding instrument between Firmaprofesional and the subscriber.
- Termination of the legal relationship between Firmaprofesional and the Subscriber.
- Modification or expiry of the underlying legal relationship or cause which allowed the issuance of the signatory's certificate, including temporary professional disqualification.
- Infringement by the certificate's applicant of the pre-agreed requirements for the application.
- Infringement by the subscriber with regard to their obligations, liabilities and guarantees established in the relevant legal document or CPS.
- Unexpected incapacity, either total or partial.
- Death of the subscriber or signatory.
- Receipt of a valid revocation request issued by the subscriber or the signatory.
- The authorization to be a payment service provider has been revoked by the ANC.

e. Other circumstances:

- Suspension of the digital certificate for a period greater than that specified in the CPS.
- Because of a legal or administrative order.
- For any other due cause specified in the CPS.

In any case, the ANC may specify in its request the reason why it requests the revocation.

4.9.2. Who can request revocation

The revocation of a certificate may be requested by:

- The signatory, who is obliged to request the revocation of the certificate if they have knowledge of any of the circumstances mentioned above.
- Any person may request revocation of a certificate if they have knowledge of any of the circumstances mentioned above.
- In case of revocation of PSD2 certificates, the revocation request can be made by the Bank of Spain or the Competent National Authority (ANC).

The certificate can be revoked by:

- The operators of the RA of the certificate subscriber.
- Authorised operators of the CA.

4.9.3. Procedures for requesting revocation

There are various options for the subscriber or signatory when requesting the revocation of a certificate.

In all cases, as soon as the certificate is suspended or revoked, a statement will be sent to the subscriber and the signatory, indicating the time and reason for the action.

4.9.3.1. Online procedure

Firmaprofesional has an online form available for the subscriber or signatory where they can request revocation of their certificate.

To do this, the subscriber must:

- Access the revocation section in the Firmaprofesional website.
- On the form provided, correctly enter their identification data.
- Enter the revocation code provided during the certificate generation process.

- Enter the reason for the revocation request.
- Explicitly accept the processing of the application and its consequences.

Once the operation has been approved, the certificate will be immediately revoked.

The RA will receive an email from the system stating that the certificate has been revoked.

4.9.3.2. Revocation during office hours

The subscriber or the signatory should contact their RA, who, in turn, must identify and authenticate their identity through whatever procedures it deems appropriate.

Once correctly identified, the operator will execute the revocation.

4.9.3.3. Revocation outside of office hours

To request the revocation of a certificate outside of office hours contact Firmaprofesional's telephonic revocation service on the following number:

- 24x7 Revocation Service: 902.361.639

As a precautionary measure Firmaprofesional will suspend the certificate within 24 hours of receiving the request for revocation, and send a message to the RA with the suspension data and reason.

The RA will have a maximum of 5 days to verify the authenticity of the revocation request and to complete, or otherwise cancel, the process of certificate revocation.

This term will be reduced to 24 hours in the following cases:

- The subscriber requests in writing that Firmaprofesional revokes the certificate.
- The subscriber notifies Firmaprofesional that they have not authorised the original certificate request and do not retroactively grant this authorisation.
- Firmaprofesional obtains proof that the subscriber private key corresponding to the public key in the certificate has been compromised.
- Firmaprofesional obtains evidence that the validation of the domain authorisation, or the control of any qualified domain name or IP address in the certificate cannot be trusted.

If at the end of this period, the certificate is still suspended, Firmaprofesional will proceed with the automatic revocation.

4.9.4. Period in which the CA must resolve the revocation request

Once the signatory's identity has been authenticated following the procedure detailed previously, and the revocation duly processed by the RA, the revocation will be effective immediately.

4.9.5. Revocation verification requirement for relying parties

Verification of the status of a certificate is obligatory for each use of a certificate, either by consulting the Certificate Revocation List (CRL) or the OCSP service.

4.9.6. Frequency of announcement of CRLs

The CRL of the end entity certificates are issued at least every 24 hours, or whenever a revocation occurs, and are valid for 7 days.

The CRL of the certificates of authority is issued every 6 months or whenever a revocation occurs.

4.9.7. Maximum time between the generation and publication of the CRLs

The publication of the CRL is performed at the same time as its generation hence the elapsed time is zero.

4.9.8. Availability of the online system for verification of the status of certificates

Information concerning the status of the certificates will be available online 24 hours a day, 7 days a week.

In case of system failure, or any other factor which is not under the control of the CA, every

effort will be made to ensure that this information service is available within a maximum of 24 hours.

4.9.9. Requirements for checking revocation online

To use the CRL service, which is open access, the following must be considered:

- In all cases the last issued CRL must be checked, this can be downloaded from the URL contained in the certificate itself in the "CRL Distribution Point" extension.
- The user should also check the CRL(s) related to the certification chain of the hierarchy.
- The user must ensure that the revocation list is signed by the authority that issued the certificate to be validated.
- Revoked certificates which expire will be removed from the CRL.

To use the OCSP service, the following must be considered:

- The revocations can be checked using GET or POST methods
- Information provided via OCSP service is updated at least every four days

4.9.10. Circumstances for suspension

Firmaprofesional may suspend a certificate in the following cases:

- If it is suspected that a key has been compromised, until this fact is confirmed or contradicted.
- If the subscriber has defaulted on a payment for their certificate.
- If all the information necessary to justify the revocation of a certificate is unavailable

4.9.11. Who can request suspension?

The suspension of the certificate can only be effected by:

- The operators of the RA of the certificate subscriber.

- Authorised operators of the CA.

4.9.12. Limits to the period of suspension

After 15 days of suspension, the CA may proceed with the revocation of the certificate.

4.10. Information services for the status of certificates

4.10.1. Operational characteristics

Firmaprofesional publishes Certificate Revocation Lists (CRLs) online, this service is free and with unrestricted access.

Firmaprofesional offers a free online certificate verification service using the OCSP protocol.

In addition, Firmaprofesional can provide a commercial certificate validation service.

4.10.2. Service Availability

Information concerning the status of the certificates will be available online 24 hours a day, 7 days a week.

In case of system failure, or any other factor which is not under the control of the CA, every effort will be made to ensure that this information service is available within a maximum of 24 hours.

4.10.3. Additional characteristics

The use of the OCSP service is public and free.

Firmaprofesional may arrange advanced certificate validation services that require a specific license.

4.11. Expiration of the Subscription

The subscription will end at the time of expiration or revocation of the certificate.

4.12. Custody and recuperation of keys

Firmaprofesional does not maintain backup copies of the subscriber's or signatory's private key neither does it offer key recovery services (key escrow).

5. PHYSICAL SECURITY, FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

5.1. Physical controls

The CA has established physical and environmental security controls to protect the resources of the facilities housing the systems and the equipment used for the operations.

The physical and environmental security measures applicable to the certificate generation and revocation services provides protection against:

- Unauthorised physical access.
- Natural disasters.
- Fires.
- Failure of the support systems (electricity supply, telecommunications, etc.)
- Collapse of the structure.
- Floods.
- Theft.
- Unauthorised removal of equipment, information, storage media and applications related to components employed for the services of the Trust Service Provider.

The facilities include systems of preventative and corrective maintenance which are monitored continuously, 24hr/day-365 days/year with an operative in attendance in the 24hrs following the warning. Since the installations are located in the centre of a provincial capital the presence of security forces is guaranteed within a period not exceeding 30 minutes.

5.1.1. Physical location and construction

The CA facilities are built with materials that guarantee protection against brute force attacks. They are located in an area of low disaster risk which permit rapid access.

Specifically, the room where the cryptographic operations are performed is a Faraday cage with protection against external radiation, double flooring, fire detection and extinguishing equipment, anti-moisture systems, a back-up cooling system and a back-up power supply system.

5.1.2. Physical access

Physical access to the premises of the Trust Services Provider, where the certification processes are carried out, is limited and protected by a combination of physical and procedural measures.

Access is limited to expressly authorised personnel, requiring identification at the time of access and registration, they may be filmed by CCTV and the recording archived.

The facilities include motion detectors in all vulnerable points and alarm systems for the detection of intruders, with warnings given via various channels.

Access to the rooms is through ID card and fingerprint readers, this is managed by a computer system which automatically maintains an entry and exit log.

5.1.3. Power supply and air conditioning

CA facilities have electrical current stabilising equipment and a backup power supply system consisting of a redundant generator with fuel tanks that can be filled from outside.

The rooms housing the IT equipment have temperature control systems equipped with a backup air conditioning system.

5.1.4. Exposure to water

The rooms housing the IT equipment have a moisture detection system.

5.1.5. Fire prevention and protection

The rooms housing the IT equipment have systems for automatically detecting and extinguishing fires.

5.1.6. Storage system

All removable storage media (tapes, cartridges, diskettes, etc.) containing classified information are labelled according to the highest level of classification of the information they contain and are only available to authorised personnel.

Information classified as *Confidential,* regardless of the storage device, is stored in fireproof or permanently locked cabinets, requiring express authorisation for its removal.

5.1.7. Removal of storage devices

When no longer useful, sensitive information is destroyed in the manner most appropriate to the device containing it:

- Hard copies and paper: paper shredders or wastepaper bins provided for this purpose and subsequently destroyed under supervision.
- Storage media: before being disposed of or reused should be erased, physically destroyed or the content made unreadable.

5.1.8. Off-site backups

The CA maintains a secure external storage site independent of the operational centre, for the safekeeping of documents, magnetic and electronic devices.

Access to the site and deposit or removal of devices requires at least two expressly authorised persons.

5.2. Procedural Controls

5.2.1. Trusted roles

The trusted roles are those described in the respective Certificate Policies of the hierarchy, they are organised so as to guarantee a division of the roles which spreads the control and minimises the possibility of internal fraud, so not allowing a single person to control all of the certification functions from start to finish .

According to the specifications of ETSI standards EN 319 401 and CEN/TS 419261, the minimum established roles are:

a. Security Officers: maintain the overall responsibility for the administration and implementation of policies and safety procedures.

b. Registration Officers: responsible for the approval, issue, suspension and revocation of End Entity certificates, as well as verification of appropriate web authentication certificates.

c. Revocation Officers: responsible for making changes to the status of a certificate.

d. System Administrators: authorised to make changes to the system configuration, but without access to its data.

e. System Operators: responsible for the day-to-day management of the system (monitoring, backups, recovery ...)

f. System Auditors: authorised to access the system logs and verify the procedures performed on it.

g. CA Operator - Certification Operator: responsible for activating the keys of the CA in the online environment, for the certificate signing processes and CRLs in the Offline Root environment.

5.2.2. Number of persons required per task

The CA guarantees at least two people to perform tasks that require multiperson control as detailed below:

- The generation of the CA's keys.
- The recovery and back-up of the CA's private keys.
- Issuing the CA's certificates.
- Activation of the CA's private keys.
- Any activity performed on the hardware and software resources that support the Root CA.

5.2.3. Identification and authentication by role

The people assigned to each role are identified by the internal auditor who ensures that each person performs their designated tasks..

Each person only controls the resources necessary for their role, so ensuring that no-one accesses unassigned resources.

Resources may be accessed, depending on the type of resource, by login/password, digital certificates, physical access cards and keys.

5.2.4. Roles requiring segregation of duties

are incompatible in time with the Certification tasks and also incompatible with Systems. These functions will be subordinated to the head of operations, reporting to them as well as to the technical management.

The Auditor's tasks are incompatible in time with the tasks of the Certification Operator and also incompatible with the Systems tasks. These functions will be subordinated to the head of operations, reporting both to them and to the technical director.

Systems Management staff may not carry out any task related to Auditing or Certification.

5.3. Personnel controls

5.3.1. Requirements for qualifications, knowledge and professional experience

All personnel who have been qualified as sufficiently trustworthy to perform tasks without

supervision must have spent at least six months working in the production centre and have a fixed employment contract.

All staff are qualified and have been fully trained to perform the operations to which they have been assigned.

Firmaprofesional executives and staff with trusted roles are free from any commercial, financial or any other type of influence that could negatively affect confidence in the services they provide.

In cases where the subscriber is acting as a registration authority, the professional association/ public administration, institution or public legal entity/company concerned, designates from among its staff the person authorised to carry out the registration tasks. This appointment is made by the person responsible for the certification service, as previously identified in the contract to provide electronic certification services.

The registration employee will have completed a preparatory course for the tasks of registration and validation of the requests. At the end of this course, an external auditor will assess their knowledge of the process.

Firmaprofesional will remove any employee from their trusted tasks if there is evidence of any criminal act that could affect the execution of these tasks.

5.3.2. Procedure for background checks

Firmaprofesional performs appropriate checks before hiring anyone.

Being responsible for the actions of persons they authorise, the RAs can impose different criteria.

5.3.3. Training requirements

Firmaprofesional provides the courses necessary to ensure the successful completion of the certification tasks, especially when substantial changes are made to them and dependent on the personal knowledge of each operator.

5.3.4. Requirements and frequency of training updates

Updates will be made on an annual basis, except for changes to the CPS, which will be

notified as they are approved.

5.3.5. Task rotation frequency and sequence

No additional stipulation.

5.3.6. Sanctions for unauthorised actions

Firmaprofesional has an internal disciplinary system for penalising unauthorised actions, with the authority to terminate employment.

5.3.7. Requirements for contracting third parties

Employees contracted to perform trusted tasks must first sign confidentiality clauses and also the operational requirements used by the CA. Any action which compromises the security of the accepted critical processes may lead to the termination of the employment contract.

5.3.8. Documentation supplied to personnel

Firmaprofesional makes documentation available to all personnel describing their assigned functions, policies and practices governing these processes as well as the security documentation.

In addition, to help carry out their duties competently documentation required by personnel will be provided at any time.

5.4. Procedures for the security audit

5.4.1. Types of event recorded

Firmaprofesional records and stores the logs of all events related to the CA's security system. These include the following events:

- Switching the system on and off.
- Attempts to create, delete, set passwords or change privileges.

- Attempts to start and end the session.
- Unauthorised attempts to access the CA's system via the network.
- Unauthorised attempts to access the CA's internal network.
- Unauthorised attempts to access the file system.
- Physical access to the logs.
- Changes in the configuration and maintenance of the system.
- Records of the applications to the Certification Authority.
- Switching the CA application on and off.
- Changes in the details of the CA and/or their keys.
- Changes in the creation of certificate profiles.
- Generation of one's own keys.
- Events in a certificate's life cycle.
- Events associated with the use of the CA's cryptographic device.
- Records of the destruction of media containing keys and activation data.

In addition Firmaprofesional records:

- Changes in the security policy.
- System crashes.
- Hardware failures.
- Activities of the firewalls and routers.
- The documentation submitted by the applicant and all the information for the registration process.
- All events related to the preparation of the QSCD devices.

Firmaprofesional keeps, either as hard copies or electronically, the following information:

- The ceremonies for the key creation of the CAs and the databases for key

management.

- Physical access records.
- Maintenance and configuration changes to the system.
- Changes in personnel performing trust tasks in the CA.
- Agreement and discrepancy reports.
- Records of the destruction of material containing information on keys, activation data or personal subscriber information, if this information is managed.
- Possession of activation data, for operations with the private key of the CAs.

Only persons authorised by Firmaprofesional have access to this documentation.

5.4.2. Frequency of processing audit logs

To determine whether any suspicious or unusual activity has taken place audit logs are reviewed every week and also whenever a system alert occurs, caused for example by an incident.

5.4.3. Retention period of the audit logs

To ensure system security audit log information will be stored for 15 years.

5.4.4. Protection of the audit logs

The systems logs are protected from tampering by the signing of the files that contain them.

They are stored in fireproof devices.

Their availability is protected through storage in facilities separate to where the Certification Authority is located..

The devices are handled at all times by authorised personnel.

5.4.5. Backup procedures for audit logs

Firmaprofesional has an adequate backup procedure so that, in case of loss or destruction of

important files, the corresponding backup copies of the logs will be available in a short period of time.

The CA has implemented a secure procedure for the backup of audit logs, making a weekly copy of all the logs on external media. The external media is stored in a fireproof cabinet using security measures that ensure access is allowed only to authorised personnel. Daily incremental copies and weekly full copies are made.

Additionally a copy of the audit logs is safeguarded in an external facility.

5.4.6. Audit information collection system

Event audit information is automatically collected internally by the operating system and by the certification software.

5.4.7. Vulnerability assessments

In accordance with the internal procedure established for this purpose in the security policies, the CA performs periodic reviews of discrepancies in the information in the logs and of suspicious activity, as well as vulnerability assessments of internal and external IP addresses.

5.5. Archive of records

5.5.1. Types of event archived

Events are stored that occur during the life cycle of the certificate, including the certificate renewal. The CA will store, or delegate the RA to store, the following:

- all the audit data,
- all data related to the certificates, including the contracts with subscribers and their identification data,
- requests for the issue and revocation of certificates,
- all the certificates issued or published,
- CRL's issued or records of the status of generated certificates,

- documentation required by the auditors and
- the communications between the components of the PKI.

The CA is responsible for the correct storage of all this material and documentation.

5.5.2. Period for the conservation of records

All system data related to the lifecycle of the certificates will be kept for the period specified by the current law, whenever it is applicable. Certificates will be kept in the repository for at least one year after their expiration. The contracts with the subscribers and any information concerning the identification and authentication of subscribers will be retained for at least 15 years (from the time of expiry of the certificate) or the period established by the applicable legislation.

5.5.3. Protection of the archive

In cases where this is required, the CA ensures proper protection of the archives by assigning qualified personnel for their treatment and storage in secure, fireproof boxes in external installations.

The CA has technical and configuration documents which detail all measures taken to ensure the protection of the archives.

5.5.4. Procedures for archive backup

The CA has an external storage centre to ensure the availability of copies of the archive of electronic files. The physical documents are stored in safe places with access permitted only to authorised personnel.

5.5.5. Requirements for time-stamping of records

Records are dated using a reliable source.

The technical and configuration documentation of the CA contains a section on setting times for the equipment used in issuing certificates.

5.5.6. Archive system for audit information

Not stipulated.

5.5.7. Procedures to obtain and verify archived information

During the audit required by this CPS, the auditor will verify the integrity of the archived information.

Only authorised personnel may access the archived information.

The CA will provide the auditor with the information and the means to verify the archived information.

5.6. CA Rekeying

5.6.1. Root CA

Before the certificate of the Root CA expires a change of key (rekeying) will be made and, if appropriate, changes will be made to the content of the certificate to fit better with current legislation, the current state of Firmaprofesional and the market. The old CA and its private key will only be used for signing CRLs while there are active certificates issued by the former CA. A new CA will be generated with a new private key.

The technical and security documentation of the CA details the CA rekeying process.

5.6.2. Subordinate CA

In the case of subordinate CAs, certificate renovation can be carried out with or without rekeying. The procedure described in the previous point will only be applied in the case of rekeying.

5.7. Disaster Recovery Plan

5.7.1. Procedures for the management of incidents and vulnerabilities

The CA has developed a contingency plan, detailed in the "Security Policy" document, for the recovery of all systems in less than 48 hours, while the revocation and publication of information on the status of certificates is guaranteed in less than 24 hours.

Any failure in achieving the goals set out in the contingency plan will be treated as reasonably unavoidable, unless such failure is due to a breach of the obligations of the CA to implement the stated processes.

5.7.2. Alteration of hardware resources, software and/or data

In the event of an incident which alters or corrupts hardware resources, software or data, Firmaprofesional will proceed in the manner described in the "Security Policy" document .

5.7.3. Course of action in case of vulnerability of a CA's private key or of the cryptographic suite

The Continuity Plan of the Firmaprofesional hierarchy treats the compromise of a CA's private key or of the cryptographic suite (algorithms) as a disaster.

In the event that a CA's private key is compromised, Firmaprofesional will:

1. Inform all subscribers, users and other CAs with which it has agreements or any other type of formal commitment, at least by posting a warning on the CA's webpage.
2. The warning will indicate that any certificates and information concerning the status of revocations signed using this key or algorithms are invalid.
3. The national supervisor will be notified within 24 hours after the compromise has been discovered.
4. Revoke, within the period agreed with the national supervisor, the certificates issued by this CA, applying, if applicable, any of the procedures provided in the Plan of Cessation or the Continuity Plan

5.7.4. Business continuity following a disaster

Within 24 hours of a disaster or unforeseen emergency the CA will restore the critical services (revocation and publication of revoked certificates) in accordance with this CPS, basing its actions on the contingency plan and continuity of existing business plan.

If necessary, the CA has an alternative centre, for the operation of the certification systems.

5.8. Termination of activity

5.8.1. Certification Authority

Before ceasing its activity the CA will carry out the following actions:

- Whenever necessary, it will provide the funds required (by means of civil liability insurance) to finalise any revocation activities until the definitive cessation of the activity.
- A minimum of 2 months notice of the cessation, or the period required by the legislation in force at the time, will be given to all subscribers, applicants, users, other CA's or entities with which the CA has agreements or any other type of relationship.
- It will revoke any authorisation to subcontracted entities to act on behalf of the CA in the certificate issuing process.
- In accordance with Article 21 of Law 59/2003 on electronic signatures, the CA may transfer, with the express consent of the subscribers, the management of the certificates that remain valid on the date of the cessation to another trust service provider which will assume responsibility for them, or otherwise terminate their validity. When applicable the CA will provide information on the characteristics of the TSP to which it proposes transferring the management of the certificates.
- It will inform the competent authorities, with the required advance notice, of the cessation of its activity and the destination to be given to the certificates, specifying, where appropriate, whether to transfer the management and to whom.
- Prior to the definitive cessation of the activity, the competent authorities will be informed regarding the qualified certificates issued to the public whose validity has been extinguished so that they can take custody in accordance with Article 20.1.f)

of Law 59/2003.

- It will inform the competent authorities, of the opening of any insolvency proceedings instituted against Firmaprofesional as well as any other relevant circumstances that may prevent the continuation of the activity.
- Firmaprofesional indicates in its plan for cessation of service what information will be returned.

5.8.2. Registration Authority

Before the cessation of a registration authority of a specific group, Firmaprofesional will:

- Stop issuing and renewing certificates of this RA.
- Revoke the operator certificates of this RA.
- Revoke the subscriber certificates issued by this RA, unless it has been expressly decided not to do so.

In its turn the RA will:

- Deliver to Firmaprofesional all documentation associated with the issue and management of certificates, whether in paper, electronic or any other format.

6. TECHNICAL SECURITY CONTROLS

6.1. Key pair generation and installation

6.1.1. Key pair generation

The key generation of the CAs is performed, according to the documented key ceremony process, on Hardware Security Modules (HSM) located within the security room of the CSP. It is carried out by staff deemed appropriate according to their trusted roles and, with at least one dual control and witnesses from Firmaprofesional, the head organisation of the CA and the external auditor.

Firmaprofesional guarantees that the CA's signing keys are not used for any purpose other than those indicated in this document.

For end entity certificates, key generation devices will be carried out on devices which provide reasonable assurance that the private key can only be used by the signatory, either by physical means or by the subscriber setting the controls and afterwards taking appropriate security measures.

In cases where Firmaprofesional can guarantee that the cryptographic keys of the signatory were created on a Qualified Signature Creation Device (QSCD) that meets the requirements set out in Art. 24 of Law 59/2003 on Electronic Signatures and Annex II of the Regulation (EU) 910/2014, it will be indicated on the certificate itself by including the corresponding OID identifier in the "Certificate Policies" extension.

In any other case, for example, if the private keys have been generated in an Internet browser, certificates will be issued with a different OID identifier.

6.1.2. Private key delivery to the signatory

The RA is responsible for ensuring the delivery of the certificate to the signatory, whether by delivering the signature device or making available the means for its download and subsequent use, ensuring that the signatory is in possession of the signature creation data corresponding to the verification data which appears in the certificate.

6.1.3. Private key delivery to the certificate issuer

Sending the public key to the CA for certificate generation is done using a standard format, preferably in PKCS # 10 or self-signed X.509, using a secure channel for the transmission.

6.1.4. CA public key delivery to relying parties

The certificate of the CA of the chain of certification and their fingerprint will be available to users on the website of Firmaprofesional.

6.1.5. Key sizes

Certificate	RSA Key size (bits)	Period of validity (years)
Root CA	4096	21
Subordinate CA	2048	21
End entity	2048	As established in the legislation and current regulations
Operator / Administrator	1024 / 2048	5 (maximum)

The migration of all keys of length 1024 bits to 2048 bits is currently in progress.

6.1.6. Public key parameters generation and quality checking

The parameters recommended in the technical specifications document ETSI TS 119 312 are used.

Specifically the parameters used are the following:

Signature Suite	Hash Function	Padding Method	Signature algorithm
sha256-with-rsa	sha256	emsa-pkcs1-v1.5	rsa

6.1.7. Acceptable key usage (as per the Key Usage Field of X.509 v3)

All certificates include the extension *Key Usage* and *Extended Key Usage*, indicating authorised uses of the key.

Permitted uses of the key for each certificate are defined in the corresponding Certification Policy.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic module standards

The cryptographic modules used to generate and store the keys of the Certificate Authorities are certified with the FIPS-140-2 standard Level 3.

The keys of subscribers with certificates qualified by QSCD and of operators and administrators are securely generated by the individual themself using a qualified device which is compliant with Implementing Decision (EU) 2016/650 of the Commission of 25 April 2016, which specifies the rules for the evaluation of the security of the Qualified Signature (or Seals) Creation Device in agreement with Article 30, paragraph 3, Article 39, paragraph 2, and Article 51.1 of Regulation (EU) No. 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

Firmaprofesional verifies that the cryptographic devices (QSCD) employed by either Firmaprofesional or the subscriber comply with the appropriate regulations and current legal requirements. This verification is repeated over time.

6.2.2. Private key (m out of n) multi-person control

Access to private keys of the CA requires the simultaneous participation of two different cryptographic devices out of a possible five, protected by a password.

6.2.3. Custody of the private key

The private key of the root CA is guarded by a cryptographic hardware device certified according to FIPS 140-2 Level 3, ensuring that the private key is never visible outside of the cryptographic device. Activation and use of the private key requires the multiperson control detailed above. The session is closed after the operation has been performed, so disabling the private key.

The private keys of the Subordinate CAs are guarded on secure cryptographic devices certified according to FIPS 140-2 Level 3.

Firmaprofesional does not maintain backup copies of the private key of subscriber's certificates (*key escrow*).

If the subscriber guards the private keys of the signatory, it must be performed using secure cryptographic devices certified according to the information given in Section 6.2.1 and guaranteeing at all times that the signatory has exclusive use of the keys.

6.2.4. Private key backup

There are devices that allow the restoration of the CA's private key, which are stored securely and are accessible only to personnel authorised according to their trusted roles, using at least one dual control in a secure physical environment.

The keys of the Root CA and Subordinate CA can be restored by a process which requires the simultaneous use of 2 out of 5 cryptographic devices (cards).

This procedure is described in detail in Firmaprofesional's security policies.

6.2.5. Private key archival

The CA will not archive the private signing key for certificates after the expiration of their validity period.

The private keys of the internal certificates used by the distinct components of the CA's system to communicate with each other, to sign and to encrypt the information will be archived for a period of at least 10 years after the last certificate has been issued.

6.2.6. Private key transfer into or from a cryptographic module

There is a CA key ceremony document which describes the processes for generating the private key and the use of the cryptographic hardware.

6.2.7. Method for activating the private key

The keys of the Root CA are activated by a process which requires the simultaneous use of 2 out of 4 cryptographic devices (cards).

The keys of the Subordinate CA are activated by a process which requires the use of 1 out of 4 cryptographic devices (cards).

6.2.8. Method of deactivating the private key

Each time the application restarts the private keys are automatically disabled

6.2.9. Method of destroying of the private key

Devices that have stored any part of the private key for signing the CA's certificates, or any of their activation data, are physically destroyed or reset to low level. This includes devices containing copies of these keys.

6.3. Other aspects of key pair management

6.3.1. Archive of the public key

The CA will keep all public keys during the period required by the existing law, where applicable, or while the certification service is active and otherwise a minimum of 6 months.

6.3.2. Periods for certificate operation and key pair usage

The period of use of a certificate will be determined by its period of validity.

A certificate should not be used after its period of validity, although the relying party can use it to verify historical data, taking into account that there will be no online verification service

valid for that certificate .

6.4. Activation data

6.4.1. Activation data generation and installation

Activation data is generated at the time of initialisation of the cryptographic device.

If the initialisation occurs in an external entity, the activation data will be delivered to the subscriber through a process that ensures confidentiality with respect to third parties.

6.4.2. Activation data protection

Only authorised personnel have knowledge of the activation data of the private keys of the Root CA and Subordinate CA.

For end entity certificates, once the device and activation data have been delivered, it is the responsibility of the subscriber or signatory to maintain the confidentiality of this data.

6.5. Computer security controls

The CA uses reliable systems and commercial products to provide its trust services.

The equipment used is initially configured, by the systems personnel of Firmaprofesional with the appropriate security profiles, with the following aspects:

- Security configuration of the operating system.
- Security configuration of the applications.
- Correct sizing of the system.
- Configuration of users and permissions.
- Configuring of the events log.
- Backup and recovery plan.
- Antivirus settings.

- Network traffic requirements.

Firmaprofesional's technical and configuration documentation details the architecture of the equipment providing the certification services, in terms of both physical and logical security.

6.5.1. Specific security technical requirements

Each server of the CA includes the following features:

- Access control to the CA services and privilege management.
- Imposition of separation of duties for the management of privileges.
- Identification and authentication of roles associated with identities.
- Archive of the history file of the subscribers, the CA and the audit data.
- Audit events related to security
- Self-diagnosis of security related to the CA services.
- Mechanisms for recovery of keys and the CA system.

The functionalities listed above are provided through a combination of the operating system, PKI software, physical protection and procedures.

6.5.2. Evaluation of the computer security

The security of the equipment is assessed by an initial risk analysis in such a way that the security measures are instituted in response to the probability and impact produced when a group of defined threats exploit security breaches.

Physical security is guaranteed by the previously described facilities. Due to the small number of people carrying out their jobs in the data centre of Firmaprofesional management of personnel is relatively simple.

6.6. Life cycle security controls

6.6.1. System development controls

The CA has a procedure to control the changes in versions of the operating systems and applications indicating an improvement in its security features or other features to correct detected vulnerabilities.

6.6.2. Security management controls

6.6.2.1. Security management

The CA carries out specific activities for the training and awareness of employees on security matters. The materials used for the training and documents describing the processes are updated after approval by a security management panel.

The CA requires, by contract, security measures equivalent to any external provider involved in certification tasks.

6.6.2.2. Classification and management of information and property

The CA keeps an inventory of assets and documentation and follows a procedure to ensure the correct use and management of this material.

The CA security policy details the procedures for the management of the information, where it is classified according to the level of confidentiality.

The documents are categorised into three levels: PUBLIC, INTERNAL AND CONFIDENTIAL.

6.6.2.3. Management operations

The CA has an adequate procedure for management and response to incidents, through the implementation of a system of alerts and the generation of periodic reports. The process for incident management is detailed in the technical documentation of the CA and the Datacentre procedures.

The CA has fireproof security boxes for storing physical media.

The whole procedure concerning the functions and responsibilities of personnel involved in the control and manipulation of the components of the certification process is documented by the CA.

6.6.2.4. Treatment of the storage devices and security

All storage media will be treated securely in accordance with the requirements of the classification of information. Media containing sensitive data are destroyed in a secure manner if they will not be required in the future.

6.6.2.5. System planning

The technical department of the CA keeps a record of the equipment capabilities .

Using the application of resource control for each system, it is possible to make provision for a possible resizing.

6.6.2.6. Incident reports and responses

The CA has a procedure for the monitoring of incidents and their resolution where responses and an efficient evaluation, which supposes the resolution of the incident, are recorded.

6.6.2.7. Operational procedures and responsibilities

The CA defines the activities assigned to people with a trusted role in a different way to persons responsible for performing daily operations of a non-confidential nature.

6.6.2.8. Management of the access system

The CA makes every reasonable effort, within its reach, to ensure that access to the system is limited to authorised persons. In particular:

a. General management of the CA:

- Controls are available based on high availability firewalls.

- Sensitive data is protected by cryptographic techniques or access controls with strong authentication.
- The CA has a documented procedure for managing the activation and deactivation of users and access policy. This is detailed in its security policy.
- The CA has a procedure to ensure that operations are conducted in compliance with the roles policy.
- Each person has their associated identifier to carry out certification operations according to their role.
- CA personnel will be responsible for their actions, for example, for retaining event logs.

b. Certificate generation:

- The CA's facilities are equipped with continuous monitoring systems and alarms to detect, record and allow immediate action against any unauthorised and/or irregular attempt to access resources.
- The authentication for the issuing process is performed by a system requiring the presence of m out of n operators to activate the private key of the CA.

c. Revocation management:

- The CA's facilities are equipped with continuous monitoring systems and alarms to detect, record and allow immediate action against any unauthorised and/or irregular attempt to access resources of the revocation system.
- Revocation refers to the permanent loss of effectiveness of a digital certificate. The revocation will be made by strong authentication with a card using the software of an authorised administrator. The log systems will generate tests that guarantee non-repudiation of the action taken by the CA operator.

d. Revocation status

- The application for of the status of the revocation offers access control based on authentication by certificate to prevent any attempt to change the information on the status of the revocation.

6.6.2.9. Management of the life cycle of the cryptographic hardware

- The CA ensures that the cryptographic hardware used for the signing of certificates is not tampered with during its transport.
- Cryptographic Hardware is made with storage media prepared to avoid any tampering.
- The CA records all relevant device information to add to the catalog of assets of Firmaprofesional, SA
- The use of cryptographic hardware for certificate signing requires the use of at least two trusted employees.
- Firmaprofesional carries out periodic tests to ensure the correct operation of the device.
- The cryptographic device is only handled by trusted employees.
- The CA's private signing key stored in the cryptographic hardware will be deleted once the device is retired.
- The system configuration of the CA, as well as its modifications and updates are documented and controlled.
- To ensure proper device maintenance the CA has a maintenance contract. Changes or updates are authorised by the security officer and are reflected in the corresponding work records. These settings are made by at least two trusted employees.

6.7. Network security controls

The CA prevents physical access to network management devices and has an architecture that directs the traffic generated based on its security features, creating clearly defined network sections. This division is performed by using firewalls.

Confidential information which is transferred by unsecured networks is encrypted.

6.8. Time source

Time is obtained via specific hardware with a rubidium atomic clock, GPS synchronisation and through consulting the Real Observatorio de la Armada (Royal Naval Observatory)[5], following the NTP protocol over the Internet. A description of the NTP protocol can be found in RFC 5905 "Network Time Protocol".

[5] Website information:
http://www.armada.mde.es/ArmadaPortal/page/Portal/ArmadaEspannola/ciencia_observatorio/06_Hora

7. CERTIFICATE, CRL AND OCSP PROFILES

7.1. Certificate profile

The profile of the certificates corresponds with that proposed in the relevant certification policies, and are consistent with those set out in the following standards:

- ETSI 319 412: Electronic Signatures and Infrastructures (ESI); Certificate Profiles
- RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile",
- RFC 3739 "Qualified Certificates Profile".

The following features are common to all the certificates:

Certificate Field	Name	Description
Version	Version Number	V3 (standard version X509)
Serial	Serial Number	Unique random code with respect to the issuer's DN
Issuer	Issuer	DN of the CA issuing the certificate
notBefore	Valid from	Start date of validity, UTC
notAfter	Valid until	End date of validity, UTC
Subject	Subject (DN)	Distinguished Name of the subscriber
Extensions	Extensions	Extensions of the certificates

7.1.1. Version number

The certificates follow standard X.509 version 3.

7.1.2. Certificate extensions

Extension	Critical	Possible Values
X509v3 Basic Constraints	Yes	2 possible values depending on whether it is treated as a CA certificate CA:FALSE CA:TRUE
X509v3 Key Usage	Yes	Digital Signature Content Commitment Key Encipherment

		Data Encipherment Key Agreement
X509v3 Extended Key Usage	-	Variable dependent on certificate type
X509v3 Subject Key Identifier	-	ID of the certificate's public key obtained from its own hash
X509v3 Authority Key Identifier	-	ID of the CA certificate's public key obtained from its own hash
X509v3 CRL Distribution Points	-	URI of the CRL
X509v3 Certificate Policies	-	OID of Firmaprofesional's own certification policy corresponding to the certificate URI of the CPS User Notice: Text note which can be displayed on the user's screen When applicable, OID of the European policy When applicable. OID of the Spanish policy (of public officer or legal representative, etc.)
QcStatements	-	Variable dependent on certificate type
X509v3 Subject Alternative Name	-	(optional) email of the signatory
X509v3 Issuer Alternative Name	-	(optional) URI:http://www.firmaprofesional.com
X509v3 Authority Information Access	-	URI where the CA certificate is found URI of the OCSP service

The extensions presented here correspond to all the options that issued certificates can contain. For historical and compatibility reasons, some issued certificates contain obsolete extensions. Required extensions for each certificate type are specified within the document "Certificate Profiles".

7.1.3. Object identifiers (OID) of the algorithms used

OID	Name	Description
1.2.840.113549.1.1.1	rsaEncryption	OID of the public Key
1.2.840.113549.1.1.5	sha1withRSAencryption	OID of the signing algorithm
1.2.840.113549.1.1.11	sha256withRSAencryption	OID of the signing algorithm

Firmaprofesional declares that during their validity periods the keys of the signatory or subscriber created by the CA are generated using an algorithm recognised as appropriate for the uses identified in this CPS or in the corresponding CP.

7.1.4. Name formats

The following values are common to all certificates of natural persons:

DN Field	Name	Description

CN, Common Name	Name	Name and Surnames of the signatory Additionally it can contain a numerical identification code or the NIF (Tax Identification Number) of the signatory, distinguishing the value by the previous inclusion of a label "/ num.:" o " – NIF " Additionally some types of certificate may contain the indications of use "firma", "cifrado" or "autenticación"
E, E-mail	E-mail	E-mail of the signatory
ST, State	Geographical location	Geographic area associated with the signatory
C, Country	Country	Two digit country code complying with ISO 3166-1. By default "ES"
serialNumber	Serial Number	NIF or NIE of the signatory[6] In the types of certificates where a pseudonym is used, this field is prohibited
SN, surName	Surnames	Surnames of the signatory In the types of certificates where a pseudonym is used, this field is prohibited
GN, givenName	Given Name	Given name of the signatory In the types of certificates where a pseudonym is used, this field is prohibited

7.1.5. Name restrictions

Regarding the encryption of certificates, and following the standard RFC 5280 (*"Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*"), certificates issued after April 17, 2008 employ UTF8String encryption for fields containing special characters, and *PrintableString* for the rest.

For certificates issued before this date, the fields with special characters employ *PrintableString*, extended in a non-standard manner to interpret special characters (such as accents or "ñ") according to the Latin-1 encoding.

7.1.6. Certificate policy object identifier (OID)

The OID of the CPS is the following: 1.3.6.1.4.1.13177.10.0.XY, where the last two digits (X and Y) indicate the version (major and minor respectively) of the document.

The OID of each certificate included in the certification policy for each type of certificate are

[6] If the signatory does not have a NIF or NIE, the passport number in the format indicated in the relevant section of the CPS should be used. Coding according to ETSI EN 319 412-1 is recommended.

detailed in the first chapter of this document.

7.1.7. Syntax and semantics of the "PolicyQualifier"

Two PolicyQualifiers are used in the Certificate Policies extension:

- id-qt-cps: Contains the URL where the CPS and CP can be found.
- id-qt-unotice: Text note that can be displayed on the user's screen during certificate verification.

7.1.8. Semantic processing for the extension "Certificate Policy"

The Certificate Policy extension permits the identification of the policy that Firmaprofesional associates with the certificate and where to find this policy.

It consists of 3 elements: the OID of the policy and the two PolicyQualifiers defined above.

7.2. Profile of the CRL

The profile of the CRL's corresponds to that proposed in the relevant certification policies, and with standard X.509 version 3 of the RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile". The CRLs are signed by the certificate authority that issued the certificates.

7.2.1. Version number

The CRLs issued by the CA are version 2.

7.2.2. CRL and extensions

7.2.2.1. CRL of the Root CA

FIELDS	VALUES
Version	2
CRL number	Incremental Number

Signing Algorithm	Sha2WithRSAEncryption
Issuer	Distinguished Name (DN) of the issuer
Effective date of issue	(date of issue of the CRL, UTC time)
Date of next renewal	Effective date of issue + 6 months
Authority Key Identifier	Hash of the issue key
Only contains Certificates of the user	NO
Only contains Certificates of the issuing body	NO
Certificate Revocation List (CRL) indirect	NO
Entries of the CRL	Certificate serial number Revocation date Reason code

7.2.2.2. CRL of the subordinate certification authorities

FIELDS	VALUES
Version	2
CRL number	Incremental number
Signing Algorithm	Sha2WithRSAEncryption
Issuer	Distinguished Name (DN) of the issuer
Effective date of issue	(date of issue of the CRL, UTC time)
Date of next renewal	Effective date of issue + 7 days
Authority Key Identifier	Hash of the issue key
Only contains Certificates of the user	NO
Only contains Certificates of the issuing body	NO
Certificate Revocation List (CRL) indirect	NO
Entries de la CRL	Certificate serial number Revocation date Reason code

7.3. Profile of the OCSP

The OCSP profile is specified in document "Certificate profiles", section 5.

OCSP services comply with the IETF RFC 6960 standard.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1. Frequency of audits

Periodic audits are carried out, usually on an annual basis.

8.2. Qualification of the auditor

Audits can be either internal or external. In this latter case they are carried out by companies well known in the auditing field.

In the case of external compliance audits of eIDAS, Firmaprofesional will perform them with a CAB (Conformity Assessment Body).

For audits of compliance with the CA / Browser Forum requirements, Firmaprofesional will perform them with an organization accepted by the Mozilla Foundation for this purpose.

In the future Firmaprofesional may establish other auditing criteria for the activity of the CA, from among those commonly accepted in the market or by establishing criteria according to current legislation.

8.3. Relationship between the auditor and the audited authority

The companies that perform the external audits never have any conflict of interest which could undermine their performance in their relationship with Firmaprofesional.

However, Firmaprofesional carries out periodic internal audits of the CA of the hierarchy to ensure its compliance at all times to the requirements set out by the certification policies of the hierarchy.

8.4. Aspects covered by the controls

The audit will verify the following principles:

a) **Publication of information:** that the CA makes public the Business Practices and Certificate Management (this CPS) as well as the policy of privacy of information and

protection of personal data and ensures its services are in accordance with these statements..

b) **Service integrity.** That the CA exercises effective controls to provide reasonable assurance that:

- The subscriber information is properly authenticated (for the registration activities performed by the CA), and
- The integrity of the keys and the managed certificates and their protection throughout the whole of their lifecycle.

c) **General controls**. That the CA exercises effective controls to provide reasonable assurance that:

- The information of subscribers and users is restricted to authorised users and protected from any uses not specified in the published business practices of the CA.
- The continuity of operations related to the management of the life cycle of the keys and certificates is maintained.

The tasks of use, development and maintenance of the CA's systems are properly authorised and performed to maintain their integrity.

8.4.1. Audit of the Registration Authorities

Registration Authorities with access to the software provided by Firmaprofesional for certificate management are audited by a third party prior to their implementation. In addition, audits will be carried out to verify compliance with the requirements demanded by the certification policies for the implementation of the registration work as set out in the signed service contract. The frequency of audits is determined by agreement between Firmaprofesional and the Registration Authority, always accounting for the planned activities of the Registration Authority with regard to the number of certificates or specific security requirements..

However, as an exception, Firmaprofesional could exempt a Registration Authority from the obligation to undergo an initial audit and from the maintenance audits.

8.5. Actions to take as a result of incident detection

Whenever incidents or non-conformities are detected, appropriate measures for their resolution will be undertaken in the shortest time possible. For severe non-conformities

(affecting critical services, namely REVOCATION SERVICES, ACTIVATION SERVICES/ CERTIFICATE SUSPENSION, CRL PUBLICATION SERVICES), Firmaprofesional is committed to their resolution within a maximum period of three months.

In every case a resolution committee will be formed, comprising personnel from the affected areas and also a follow-up committee formed by those responsible for the affected areas and the Executive Management.

8.6. Reporting of results

The auditor shall pass on the results to the Technical Director and the Director-General, as well as the person with ultimate responsibility in Firmaprofesional.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. Fees

9.1.1. Fees for issuing or renewing certificates

The sales department of Firmaprofesional will inform clients, or potential clients of the prices for the certification service or any other service.

9.1.2. Certificate access fees

Access to the issued certificates is free of charge. However the CA retains the right to impose a fee in certain cases such as the download of large quantities of certificates or any other circumstance which the CA judges appropriate to charge for.

9.1.3. Fees for access to information on status or revocation

Firmaprofesional provides free access to information on the status of certificates or revoked certificates through the publication of the relevant CRL and the OCSP service.

Firmaprofesional provides other commercial certificate validation services, fees will be negotiated with each customer for these services.

9.1.4. Fees for other services

Applicable fees for other services may be negotiated between Firmaprofesional and the clients.

9.2. Financial responsibilities

As a Certification Services Provider Firmaprofesional has sufficient financial resources to bear the risk of liability for loss or damage to users of its services and to third-parties, guaranteeing its responsibilities in its activity of TSP as required by the current Spanish legislation.

The aforementioned guarantee is established by a Civil Liability insurance with a coverage of € 3,000,000.

Such guarantees do not apply to certificates that are not recognised, in that case the amount in respect to loss or damage that must be paid by legal order is limited to a maximum of 6,000 €.

9.3. Confidentiality of information

Firmaprofesional has an appropriate policy for information processing and for the agreement forms which must be signed by all persons with access to confidential information.

Firmaprofesional complies in all cases with the current legislation on data protection and specifically with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

9.3.1. Scope of confidential information

All information that is not expressly classified as public Firmaprofesional deems as confidential. It will not disseminate any information classified as confidential without the express written

consent of the entity or organisation that has classified it as confidential, unless there is a legal order.

9.3.2. Non-confidential information

The following information will be considered non-confidential:

- The content of the present CPS.
- The content of the different Certification Policies (CP).
- The content of the different PKI Disclosure Statements (PDS).
- The information contained in the certificates, given that the subscriber previously consented for their issue, including the different statuses or conditions of the certificate.
- The Certificate Revocation Lists (CRLs), as well as any other information on the revocation status.
- The information contained in the certificate's deposits.
- Any information whose disclosure is required by regulation.

9.3.3. Responsibility to protect confidential information

Firmaprofesional is responsible for taking the appropriate measures for the protection of confidential information.

9.4. Protection of personal information

9.4.1. Protection policy for personal data

In compliance with the requirements set out in applicable regulations in the field of protection of personal data, Firmaprofesional has the Records of Processing Activities of personal data, contained in "BBDD CERTIFICADOS" file, whose purpose is the management of issued certificates and the provision of the associated certification services.

9.4.1.1. Aspects covered

The present document describes the procedures, requirements and obligations regarding the collection and management of personal data, complying with the provisions of current regulations on the protection of personal data and the applicable security measures.

Specifically, the following sections contained in Title VIII *"De las medidas de seguridad en el tratamiento de datos de carácter personal"* ("on the security measures for the treatment of personal data") of Royal Decree 1720/2007 are met in the specified sections of this document and in the Security Policy document:

a) Scope of implementation of the security document → section 9.4

b) Applicable level of security → sections 5, 6 and 9.4

c) Functions and responsibilities of personnel → section 5.3

d) Structure of the personal data files → section 9.4

e) Notification and management of incidents → Security Policy

f) Backup and recovery → Security Policy

Consequently it complies with Article 19.3 of Law 59/2003, of 19 December, on electronic signatures, which regards the certification practice statement as a security document for the purposes specified in the legislation on the protection of personal data.

9.4.2. Information treated as private

In accordance with the provisions of Article 4 of General Data Protection Regulation (GDPR), any information concerning identified or identifiable natural persons is considered personal data.

Personal information not to be included in the certificates or in the recommended mechanism for verifying the status of certificates is considered personal information of a private nature.

The following data is considered in all cases to be of a private nature:

- Applications for certificates, approved or denied, as well as any other personal information obtained for the issuing and maintenance of certificates, except the information specified in the relevant section.

- Private keys generated and/or stored by the Certification Authority.
- Any other information deemed private.

In any case, the data captured by the Certification Service Provider should be treated with the level of basic security.

9.4.2.1. Structure of personal data files

Personal field	Name and surnames
	E-mail
	Place and date of birth
	Country
	National identity number
Professional field	Tax number corresponding to the person or entity associated with the signatory
	Department or unit of the signatory
	Position, title or role in the organisation of the signatory
	Geographical location of the signatory in the organisation (company or professional association)
	Employee or professional association number

9.4.3. Information not classified as private

The following information is not classified as private:

- The information contained in the certificates, since for their issue the subscriber already consented to publication, including the different statuses or conditions of the certificate.
- The certificate revocation lists (CRLs), as well as any other information on the revocation status.

9.4.4. Responsibility for the protection of personal data

In accordance with the GDPR, confidential information is protected from loss, destruction, damage, forgery and illegal or unauthorised processing, in accordance with the requirements established in the security measures applicable by Firmaprofesional.

After any violation of security or loss of integrity that has a significant impact on the trust

service provided or related personal data, Firmaprofesional will notify the appropriate national supervisor in the field of information security or the corresponding authority for data protection, within 24 hours after learning of the incident.

9.4.5. Communication and consent to use personal data

Users must sign and accept a binding legal document to authorise the automatic processing of the personal data supplied for the provision of the agreed services, as well as the offer and contracting of other products and services of Firmaprofesional, SA.

The obtained information is used for the correct identification of users who request personalised services, for statistical studies of registered users to help improve the services provided, to perform basic administrative tasks and to communicate incidents, offers and news to registered users via email.

The personal information gathered from registered users is stored in Firmaprofesional's database which provides the necessary technical, organisational and security measures to guarantee the confidentiality and integrity of information, in accordance with the provisions of General Data Protection Regulation (GDPR), and other applicable legislation.

In any case the user will be responsible for the supplied data. Firmaprofesional reserves the right to deny service to any user who has provided false information, without prejudice to any other legal action.

At any time, any registered user may exercise the right to access, rectification, object, erasure, restriction of processing and portability of the personal data which has been supplied to Firmaprofesional by written communication including the reference "data processing".

However, if the user considers that their right to personal data protection has been violated, they will be able to register a claim towards the Spanish Data Protection Agency.

9.4.6. Disclosure related to judicial proceedings

Firmaprofesional may disclose personal data without the prior consent of the subscriber within the framework of a judicial process in compliance with a legal obligation.

9.4.7. Other circumstances for the publication of information

Those described in paragraph 1 of Article 6 of General Data Protection Regulation (GDPR).

9.5. Intellectual property rights

a. Intellectual property of the CPS

   The intellectual property of this CPS and the various CPs belongs to Firmaprofesional, SA.

b. Intellectual property of the certificates

   Unless explicitly agreed, Firmaprofesional is the only entity owning the intellectual property rights of the issued certificates.

   Firmaprofesional grants non-exclusive licenses, free of charge, to reproduce and distribute certificates, on the condition that the reproduction is complete and no element of the certificate is altered, and when necessary in relation to digital signatures and/or encryption systems within the scope of this policy. It must also be in accordance with the corresponding binding instrument between Firmaprofesional and the entity reproducing and/or distributing the certificate, as well as the corresponding conditions of issue.

c. Key properties

   The key pair is owned by the subscriber.

   The above rules appear in the binding instruments between the CAs, the subscribers and relying parties.

9.6. Obligations

9.6.1. Obligations of the CA

As set out in this document and in the regulations governing the provision of certification services, Law 59/2003 and Regulation (EU) 910/2014 of the European Parliament and of the Council, Firmaprofesional is obliged primarily:

a. To comply with the content of the current CPS, the CPs and the PDS.

b. To publish this CPS, the CPs and the PDS on their website.

c. To inform relevant subscribers, RAs and users about any modification to this CPS by publishing the modifications on their website.

d. To have a civil liability insurance covering the minimum value required by current regulations.

e. To use reliable systems for the storage of qualified certificates which permit the verification of their authenticity and prevent unauthorised persons from altering the data, restricting access in those cases or to those people indicated by the signatory and which permit the detection of any change affecting these security conditions

As far as certificates are concerned, Firmaprofesional is obliged primarily:

a. To issue certificates in accordance with this CPS and the application standards.

b. To issue certificates according to the information at its disposal, free of errors in the entered data.

c. To issue certificates whose minimum content is defined by the current regulations, when applicable.

d. Publish the issued certificates in a Register of Certificates, only when authorised by the signatory and always respecting the current regulations concerning data protection.

e. Suspend and revoke certificates in accordance with the CPS and publish these revocations in the CRL (Certificate Revocation List) and the OCSP service.

Concerning custody of information:

a. To keep information on the issued certificate for the minimum period required by current regulations, when applicable.

b. To not store or copy the Subscriber's signature creation data, whenever so required by the current regulations.

c. To protect, with due care, the signature creation data if it is in their custody.

d. To securely protect their private keys.

e. To establish mechanisms of generation and custody of information related to the

described activities, and to protect them against loss, destruction or falsification.

9.6.2. Obligations of the RA

The RA is also bound by the terms defined in the present CPS for the issuance of certificates, they are bound primarily:

a. To respect the provisions set out in the present CPS and in the CP corresponding to the type of certificate issued.

b. To respect the provisions of the contracts signed with the CA.

c. To respect the provisions of the contracts signed with the subscriber or signatory.

During the life cycle of the certificates:

a. To check the identity of the applicants for certificates according to the methods described in this CPS or by another procedure approved by Firmaprofesional.

b. To verify the accuracy and authenticity of the information provided by the subscriber or applicant.

c. Before issuing a certificate, to inform the applicant of the obligations they are taking on, the way they should safeguard the signature creation data, the procedure to be followed to report the loss or misuse of data or devices for signature creation and verification, of the price, and precise conditions for the use of the certificate, of its limitations of use and how to guarantee against possible financial liability, and the website where they can view any information concerning Firmaprofesional, CPS, the PDS and the CP corresponding to the certificate.

d. To process and deliver certificates as stipulated in the CPS, the PDS and the corresponding CP.

e. To formalise the certification contract with the subscriber in accordance with the applicable Certification Policy.

f. To pay the agreed rates for the requested certification services.

g. To archive the documents provided by the subscriber, in accordance with the period specified by the laws in force.

h. To inform the CA of the causes of revocation, always and whenever it comes to their

attention.

i. To communicate with the subscribers or signatories, by the means they consider appropriate, for the proper management of the lifecycle of certificates. Specifically, to inform them of the imminent expiration of the certificates and their suspension, rehabilitation or revocation.

j. As the personal data processor of the CA, the RA shall comply with all obligations established in Article 28 of General Data Protection Regulation (GDPR).

9.6.3. Obligations of the applicants

An applicant for a certificate is required to comply with the rules and also:

a. To provide the RA the information necessary to carry out the proper identification.

b. To make reasonable efforts, within their reach, to confirm the accuracy and veracity of the information provided.

c. To report any change in the data provided for the creation of the certificate during its period of validity.

d. To respect the provisions of the contractual documents signed with the CA and the RA.

9.6.4. Obligations of the signatories

The signatory is obliged to comply with the regulations in force and also:

a. To diligently safeguard their QSCD, private keys and secret codes.

b. To use the certificate according to the provisions of the present CPS.

c. To respect the provisions of the binding legal documents with the CA and the RA.

d. To report as soon as possible the existence of any cause for suspension or revocation.

e. To report any changes in the data provided for the creation of the certificate during its period of validity.

f. To not use the private key nor the certificate from the moment a request is made for their suspension or revocation, or they are notified by the CA or RA of a suspension or

revocation, or once the period of validity has expired.

9.6.5. Obligations of the relying parties

Users will be obliged to comply with the provisions of current legislation and also:

a. To verify the validity of certificates at the time of carrying out any operation involving those certificates.

b. To be aware of, agree to and abide by the guarantees, limits and responsibilities applicable for the acceptance and use of the trusted certificates.

c. Conocer y sujetarse a las garantías, límites y responsabilidades aplicables en la aceptación y uso de los certificados en los que confía, y aceptar sujetarse a las mismas.

9.7. Disclaimer of warranty

Firmaprofesional can refuse any warranty service that is not linked to the obligations established by Law 59/2003, of 19 December, and the Regulation (EU) 910/2014 (eIDAS).

9.8. Liabilities

9.8.1. Liabilities of the Certification Authority

In its activity of providing certification services, Firmaprofesional will take responsibility for any breaches of the provisions of the Policies and Practices of certification and, where applicable, of Law 59/2003, of 19 December, on electronic signatures and its implementation regulations, and the Regulation (EU) 910/2014 (eIDAS).

Notwithstanding the above, Firmaprofesional will not guarantee the cryptographic algorithms and standards used or be liable for damage caused by external attacks on them, provided that due diligence has been applied, according to the existing state of the art and, where applicable, undertaken in accordance with the provisions of this CPS and the Law 59/2003, of 19 December, on electronic signatures and its implementation regulations, and the Regulation (EU) 910/2014 (eIDAS).

Firmaprofesional will be liable for damage caused to the subscriber and/or signatory or any

person who in good faith relies on the certificate, provided that there is fraud or gross negligence in respect of:

- The accuracy of the information contained in the certificate on the date of issue, provided that it corresponds to authenticated information.
- Ensuring that the public and private key function together in a complementary manner.
- The correspondence between the requested and the delivered certificate.
- Any liability established by the legislation in force.

9.8.2. Liabilities of the Registration Authority

The RA will assume full responsibility in the identification procedure of subscribers and in identity verification. To do this they must proceed according to the provisions of this CPS or by another method approved by Firmaprofesional.

If the key pair generation is not performed in the presence of the subscriber, the RA will be responsible for the custody of the keys until their delivery to the subscriber.

9.8.3. Liabilities of the subscriber

It is the responsibility of the Subscriber to comply with the obligations stipulated in the present document and in the corresponding CP, and also the legally binding instrument.

9.8.4. Limitation of liabilities

Firmaprofesional will not be liable in any case where the following circumstances are encountered:

a. State of war, natural disasters, malfunction of electrical services, data transfer and/or telephonic networks or computer equipment used by the Subscriber or by third parties, or any other act of God.

b. By improper or fraudulent use of the certificate directory and CRL (Certificate Revocation List) issued by the Certification Authority.

c. For misuse of the information contained in the Certificate or CRL.

d. For the content of messages or documents signed or encrypted using the certificates.

e. With regard to actions or omissions of the Applicant and Subscriber:

- Lack of accuracy in the information provided for the certificate's issue.
- Delay in communicating the grounds for suspension or revocation of the certificate
- Absence of a request for suspension or revocation of the certificate when applicable.
- Negligence in preserving its signature creation data, in ensuring its confidentiality and in the protection of all access or disclosure.
- Using the certificate outside its period of validity, or when Firmaprofesional or the RA notify them of its revocation or suspension.
- Excess use of the certificate, in accordance with current regulations and in this CPS, in particular, in exceeding the limits stated in the electronic certificate regarding its possible uses and the individualised amount of permitted transactions or it is not used in accordance with the conditions agreed and communicated to the signatory by Firmaprofesional.

f. With regard to actions or omissions of the relying party:

- Lack of verification of the restrictions contained in the electronic certificate or this CPS with regard to their possible uses and individualised amount of permitted transactions.
- Lack of verification of the suspension or loss of validity of the electronic certificate published in the consultation service on the validity of the certificates or lack of verification of electronic signatures.

9.9. Compensation

9.9.1. Extent of the coverage

Up to the limit of the contracted coverage the insurance will take care of any amounts which Firmaprofesional SA is legally obliged to pay as a result of any legal proceedings in which it can declare its liability, arising from any negligent act, error or unintentional breach of the

current legislation among others.

9.9.2. Insurance coverage or other guarantees for the relying parties

There is no coverage for relying parties.

9.9.3. Loss limitations

Firmaprofesional limit its liability by including the limits of use of the certificate, and the limits for the value of the transactions for which they may be used, in the certificates themselves via the *qcStatements* extension (OID 1.3.6.1.5.5.7.1.3) and the corresponding CP.

If so desired and if necessary, the subscriber may request to contract a limit greater than that indicated, assuming that additional costs, if any, are agreed. In addition, the subscriber and third parties may establish between themselves specific agreements or coverage for higher value transactions, according to the applicable certification policy, maintaining in this case the limit of liability of the CA mentioned in the preceding paragraphs.

9.10. Period of validity

9.10.1. Period

The CPS, the PDS and the various CPs come into force at the moment of their publication.

9.10.2. Replacement and repeal of the CPS

This CPS, the PDS and different CPs will be repealed as soon as a new version of the document is published.

The new version will completely replace the previous document.

9.10.3. Effects of termination

For in force certificates issued under a previous CPS or CP, the new version will prevail over the previous version in all that does not directly oppose it.

9.11. Individual notices and communications with participants

Firmaprofesional establishes in the legally binding instrument with the subscriber the means and timeframe for the notifications.

Generally, the website of Firmaprofesional www.firmaprofesional.com will be used for any type of notification or communication.

In case of problems of security or loss of integrity that may affect a natural or legal person Firmaprofesional will notify them immediately about the problem.

If Firmaprofesional is notified of an email address by which the Competent National Authority can be contacted, Firmaprofesional must inform the Competent National Authority, through that email, about the way of authenticate itself to make the requests for revocation of the certificates issued under the Payment Services Directive (EU) 2015/2366

9.12. Changes in the specifications

9.12.1. Procedure for the changes

9.12.1.1. Items that can be changed without the need for notification

The only changes that can be made to this policy without requiring notification are typographic or editing corrections or changes in the contact details.

9.12.1.2. Changes with notification

The elements of this CPS can be changed unilaterally and without notice by Firmaprofesional. The modifications may be justified by legal, technical or commercial reasons.

When appropriate, the relevant Supervisory Agency will be notified of these amendments and, after final approval, the new documentation will be issued with a sufficient period of entry into force to allow the possible termination of subscribers who do not accept the changes. The time of entry into force will be widely announced at the time of publication of the changes.

9.12.1.3. Method of notification

Any proposed changes that could substantially affect subscribers, users or third parties will be notified immediately to the interested parties by publication on Firmaprofesional's website.

The RAs will be notified directly by email or phone, depending on the nature of the changes made.

9.12.2. Period and notification procedure

Affected individuals, institutions or entities may submit their comments to the organisation responsible for the administration of the policies within 45 days of the notification.

Any action taken as a result of these comments is at the discretion of the organisation responsible for the administration of the policies.

9.12.3. Circumstances under which the OID must be changed

The OID will be changed in those circumstances which alter any of the procedures described in the present document or in any of the CPs, and which directly affect the operating mode of any of the participating entities.

9.13. Claims and conflict resolution

For the resolution of any conflict that may arise in connection with this document, the CP or the binding legal document, the parties, renouncing any other jurisdiction that may apply, will submit to the "Corte Española de Arbitraje" (Spanish Court of Arbitration).

9.14. Applicable regulations

The regulations applicable to this document as well as the various CPs, and the operations arising from them, are as follows:

- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, which repeals Directive 1999/93/EC.

- Law 59/2003 of 19 December on electronic signatures.
- Law 39/2015, of October 1, on the Common Administrative Procedure for Public Administrations.
- Law 40/2015, of 1 October, of the Legal Regime of the Public Sector.
- Royal Decree 1720/2007, of 21 December, approving the Regulation implementing Organic Law 15/1999 of 13 December on the protection of personal data.
- Regulation (EU) 2016/679 of the european parliament and of the council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
- Organic Law 3/2018, of 5 December, of the protection of personal data and the guarantee of digital rights (OL 3/2018).
- Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.
- Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication.
- The current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

9.15. Compliance with the applicable regulations

Firmaprofesional states its compliance with the Law 59/2003 of 19 December, on electronic signatures, the Regulation (EU) 910/2014 (eIDAS), as well as the regulations related in previous section.

9.16. Various clauses

9.16.1. Complete acceptance clause

All relying parties accept in full the content of the latest version of this document, the PDS and the corresponding CPs.

9.16.2. Independence

The invalidity of one of the clauses contained in this CPS will not affect the rest of the document. In such a case the aforementioned clause will be void.

9.16.3. Resolution by legal means

Any controversy or dispute arising from the present document, will be ultimately settled by means of legal arbitration by an arbitrator, within the framework of the Spanish Court of Arbitration and in accordance with its Rules and Regulations, to which is entrusted the administration of the arbitration and the appointment of the arbitrator or arbitral tribunal. The parties state their commitment to comply with the given judgement.

firmaprofesional

Firmaprofesional, S.A.

August 2019