CERTIFICATION PRACTICES STATEMENT (CPS)
FIRMAPROFESIONAL, S.A.

Certification Practices statement

Version: 151005
Level: Public

WARNING: The original of this document is in electronic form on the website of Firmaprofesional: https://www.firmaprofesional.com/cps

Version History

Version	Chapter and changes
6.1	*(to see changes between previous versions, please contact with info@firmaprofesional.com)*
151005	<u>Chapter "1.3.2 Certification Authority (CA)":</u> • Constraining Subordinate CAs to which the root CA can issue certificates. • Constraining Subordinate CAs able to issue SSL, SSL EV or similar certificates. • Adding identification, clarifications and tehcnical constraints, of SHA2 certificates for the following Subordinate CAs: o Autoridad de Certificacion Firmaprofesional CIF A62634068 o AC Firmaprofesional – INFRAESTRUCTURA o AC Firmaprofesional – CFEA o AC Firmaprofesional – OTC o SIGNE Autoridad de Certificacion o SEU Autoridad de Certificacion o Santander Digital Signature <u>Chapter "Certificates for the Public Administration":</u> • Removing of "Electronic Office certificate" and moved to section "Secure Server certificates" for functional consistency. <u>Chapter "2.1 Repositories":</u> • Updating table. <u>Chapter "Registration Authority":</u> • Adding of the RA obligation to deliver to Firmaprofesional all the documentation regarding the life cycle of the certificates. <u>Chapter "6.1.5 Key size":</u> • Given the diversity of certificate policies the definition of the validity period is opened.

Table of Contents

1 INTRODUCTION

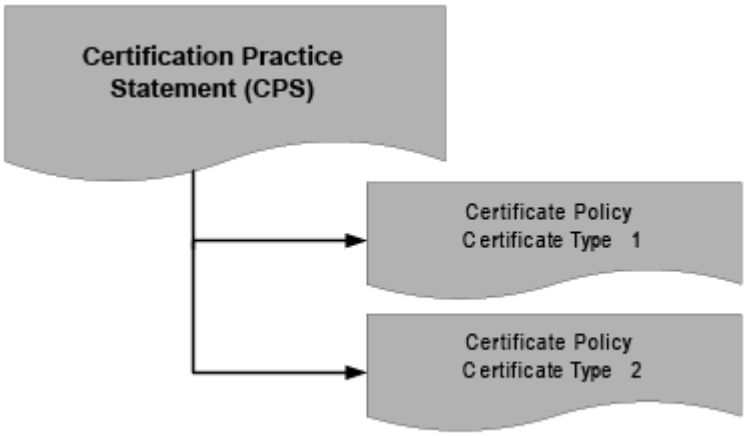
1.1 Presentation

Firmaprofesional S.A. was born as a project of several professional associations and in 2001 was established as a Public Limited Company, giving it independence of action as a Certification Services Provider (CSP) that issues qualified certificates in accordance with Law 59/2003 of 19 December on electronic signatures.

Law 59/2003 of 19 December on electronic signatures requires providers of certificate services to keep custody of and manage, on an ongoing basis, the electronic certificates which they issue. The details of this management should be set out in the Certification Practice Statement (CPS), which shall also specify the conditions governing applications for electronic certificates, their issuance and use, and the suspension and termination of their validity. The objective of the present document is to fulfil these requirements, as laid down by the Law, thereby constituting the **Certification Practice Statement** of Firmaprofesional.

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

In addition to the General Conditions outlined in this CPS, each type of certificate issued by Firmaprofesional is governed by particular conditions of issue. These conditions are set out in a document entitled "**Certificate Policy"** (CP). There is a certificate policy for each type of certificate issued.



1.2 Document Name

1.2.1 Identification

Name:	Certification Practice Statement (CPS)
Version:	151005 English Version
Description:	Certification Practice Statement of Firmaprofesional S.A.
Date of Issue:	05/10/2015
OID	1.3.6.1.4.1.13177.10.0.6.2
Location	http://www.firmaprofesional.com/cps

1.2.2 OIDs

Following digital certification standards, Firmaprofesional uses Object Identifiers (OID), as 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 is registered with IANA, registration number "**13177**", as a private enterprise OID (http://www.iana.org/assignments/enterprise-numbers).

OIDs beginning with “1.3.6.1.4.1.13177" have the following meaning:

OID	Object Type	Description
10.0.V.R	Certification Practice Statement (CPS)	V = CPS version R = CPS subversion
10.1.T.D	Certificate Policies	T = Type of Certificate 1 = Corporate certificate for professional membership organizations 2 = Corporate certificate for natural persons 3 = Web SSL Server 4 = Secure Service (VA/TSA) 5 = Corporate certificate for legal persons 6 = Corporate certificate for Electronic Invoicing 8 = Code Signing 10 = Company Seal 11 = Corporate certificate for legal representatives 20 = Electronic Office 21 = Seal for public bodies 22 = Public Employee 30 = Infrastructure certificate 40= Personal Certificate D = Device / Security Level 1 = Secure Signature-Creation Device –SSCD, DSCF in Spanish (High Level) 2 = Others Devices (Intermediate Level)
10.10.1	Subordinated CA Certificate Policy	Subordinate CA

20.0.1	Time-stamping Policy	TSA Firmaprofesional

1.3 Participating Entities

1.3.1 Certification Services Provider (CSP)

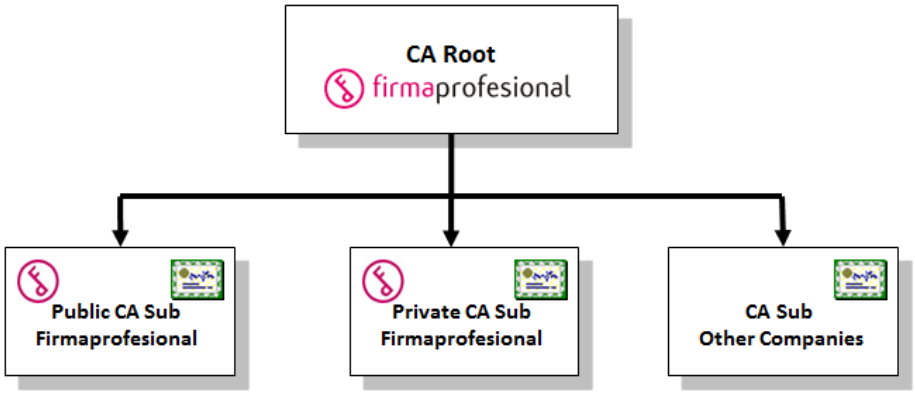
Firmaprofesional is a Certification Services Provider (CSP) which issues certificates pursuant to the Spanish Electronic Signatures Law.

Firmaprofesional is the issuing entity of the certificates and is responsible for the operations of the life cycle of the certificates. The functions of authorization, registration, issuance and revocation in respect of the personal certificates of the end-entity may be performed by other delegated entities, entered into contract with Firmaprofesional and acting as intermediaries.

Firmaprofesional also provides electronic signature and time stamp validation services; these services are governed by specific policies which are not included in this document.

1.3.2 Certification Authority (CA)

Firmaprofesional certification system is composed of various Certificate Authorities (CA) organized according to a two levels Certification Hierarchy. This hierarchy is formed by a single CA Root and various Subordinate CAs.



The Subordinate CAs may be issued to Firmaprofesional or may be issued on behalf of other Company (other Certification Services Provider – CSP -). In any case, all CAs in the Firmaprofesional Certification Hierarchy must be technically operated by Firmaprofesional and must be hosted in the infrastructure of Firmaprofesional.

The possibility that Firmaprofesional issue a subordinate CA certificate for a CSS operating with their own means, infrastructure or facilities is not authorized. So that Firmaprofesional

ensures that the technical security of all subordinate CAs is equal, regardless of the entity that appears as CSP.

If a CSP decide to operate its PKI with its own resources, Firmaprofesional will revoke the Subordinate CA certificate and a new CA will be created out of Firmaprofesional Certification Hierarchy.

Firmaprofesional can operate other PKI outside its Certification Hierarchy.

1.3.2.1 Root Certification Authority

The Root Certification Authority (*Root CA*) is the entity within the hierarchy that issues certificates to other certificate authorities, whose public key certificate has been self-signed. Its function is to sign the certificate of the other CAs belonging to the Certification Hierarchy.

There are two versions of the Firmaprofesional CA Root certificate with the same RSA 4096 bits key pair and the same identification data, one generated with the algorithm SHA1 and other with the algorithm SHA256.

The identification data of the Firmaprofesional Root Certificate are:

- ***CN: Autoridad de Certificacion Firmaprofesional CIF A62634068***
- *Hash SHA1: AEC5 FB3F C8E1 BFC4 E54F 0307 5A9A E800 B7F7 B6FA*
- *Valid from May, 20th 2.009 to December 31th 2.030*
- *Key type: RSA 4096 bits – SHA1*

- ***CN: Autoridad de Certificacion Firmaprofesional CIF A62634068***
- *Hash SHA1: 0bbe c227 2249 cb39 aadb 355c 53e3 8cae 78ff b6fe*
- *Hash MD5: 4e6e 9b54 4cca b7fa 48e4 90b1 154b 1ca3*
- *Valid from Setember 23th 2014 to May 5th 2036*
- *Key type: RSA 4096 bits – SHA-256*

Both Root CA certificates can be used interchangeably. All certificates issued by Firmaprofesional validate against both certificates. It is recommended that progressively, to the extent that the software tools allow, go replacing the SHA1 Root CA for the new SHA256 Root CA.

1.3.2.2 Public Subordinate Certificate Authorities

Delegated or Subordinate Certificate Authorities (CA Sub) are the entities within the certification hierarchy which issue end-entity certificates and whose public key certificate

has been digitally signed by the Root Certification Authority.

Certificates issued by a Public Subordinate CA can be used publicly. These certificates are regulated by different agencies (eg. Ministry of Industry -MINETUR-), recognized by different platforms (eg, Microsoft, Firefox, Chrome, Apple, Adobe, @firma, PSIS or AEAT) and audited by different standards (eg. Webtrust).

The Subordinate Certification Authority "***AC Firmaprofesional - CA1***" issues digital certificates to Private Corporations, as established by 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 25 August 2009 until 16 June 2030*
- *Key type: RSA 2018 bits – SHA1*

The Subordinate Certification Authority "***AC Firmaprofesional - AAPP***" issues digital certificates to Public Corporations, as established by Law 11/2007 of 22 June on Citizens' Electronic Access to Public Services.

- ***CN = AC Firmaprofesional - AAPP***
- *Hash SHA1: E678 37DC 4C75 EA77 458C 14C3 6B5C 0DA6 512C 6FC0*
- *Hash MD5: 742D 0EF2 4816 55CB 733B 693D FEF0 163E*
- *Valid from 7 July 2010 to 7 July 2022*
- *Key Type: RSA 2048 bits – SHA1*

Subordinate Certification Authority "***AC Firmaprofesional - CUALIFICADOS***" issue qualified digital certificates pursuant to the provisions of Law 59/2003 of 19 December on electronic signature.

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 (eIDAS) and repealing Directive 1999/93/EC*", and is issued with the algorithm SHA256:

- ***CN = AC Firmaprofesional - CUALIFICADOS***
- *Hash SHA1: 3486 ED23 6221 5545 9E9B 25FF 3F21 AD76 2798 7387*
- *Hash MD5: 5B40 65AE D107 8926 2A70 59A6 28D3 D9CA*
- *Valid from 18 September 2014 to 31 December 2030*
- *Key type: RSA 2048 bits – SHA-256*

The Subordinate Certification Authority ***"AC Firmaprofesional - INFRAESTRUCTURA"*** issues digital certificates for securing communications and services through cryptographic protocols that support PKI technology.

All SSL and SSL-EV certificates issued under the Firmaprofesional Certification Hierarchy are issued by this CA. Therefore, any other Subordinate CA under the Firmaprofesional Certification Hierarchy (public, private or to other PSC) cannot issue SSL or SSL-EV certificates.

There are two versions of this certificate with the same RSA 4096 bits key pair and the same identification data, one generated with the algorithm SHA1 and other with the algorithm SHA256. The second one is technically constrained through the use of the *Extended Key Usage* (EKU – *extKeyUsage*) extension, pursuant Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates[1] and Mozilla CA Certificate Inclusion Policy[2].

- ***CN = AC Firmaprofesional – INFRAESTRUCTURA***
- *Hash SHA1: d52f 537f 62ce 24d0 6fb5 9b0a 02bf c4a8 f7c1 6b66*
- *Hash MD5: 5735 8805 e170 28db facd d673 3b60 468f*
- *Valid from June 18th 2013 to December 31th 2030*
- *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 29th 2015 to December 31th 2030*
- *Key Type: RSA 2048 bits – SHA256*
- *Technical constrains (*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)*
  - *Time stamp signing (1.3.6.1.5.5.7.3.8)*
  - *OCSP signing (1.3.6.1.5.5.7.3.9)*

[1] Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates. CA/Browser Forum. Version 1.3.0 April 16, 2015
[2] Mozilla CA Certificate Inclusion Policy. Version 2.2

1.3.2.3 Private Subordinate Certificate Authorities

Private Subordinate Certification Authorities issue certificates for private use between entities. They are not recognized in any platform and are not regulated by any legal body.

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

The Subordinate Certification Authority "***AC Firmaprofesional – CFEA"*** issues unrecognized digital certificate for advanced electronic signature services.

There are two versions of this certificate with the same RSA 4096 bits key pair and the same identification data, one generated with the algorithm SHA1 and other with the algorithm SHA256. The second one is technically constrained through the use of the *Extended Key Usage* (EKU – *extKeyUsage*) extension, pursuant Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates[3] and Mozilla CA Certificate Inclusion Policy[4].

- ***CN = AC Firmaprofesional - CFEA***
- *Hash SHA1: 6B66 7859 C1D8 C0F6 2F20 5B21 53D3 255C 7E16 CE0B*
- *Hash MD5: EDFA 76DE 7424 F6A3 C5D1 3D06 DD67 3FF0*
- *Valid from Febrery 20th 2013 to December 31th 2030*
- *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 29th 2015 to December 31th 2030*
- *Key type: RSA 2048 bits – SHA256*
- *Technical constrains (*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)*
  - *Smartcard logon (1.3.6.1.4.1.311.20.2.2)*

The Subordinate Certification Authority "***AC Firmaprofesional – OTC***" *(OTC: one-time certificate)* issues unrecognized digital certificate for advanced electronic signature services.

[3] Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates. CA/Browser Forum. Version 1.3.0 April 16, 2015
[4] Mozilla CA Certificate Inclusion Policy. Version 2.2

These certificates are valid for a single day and will be limited to sign a single document.

There are two versions of this certificate with the same RSA 4096 bits key pair and the same identification data, one generated with the algorithm SHA1 and other with the algorithm SHA256. The second one is technically constrained through the use of the *Extended Key Usage* (EKU – *extKeyUsage*) extension, pursuant Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates[5] and Mozilla CA Certificate Inclusion Policy[6].

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

- ***CN = AC Firmaprofesional - OTC***
- *Hash SHA1: 6e 13 b5 1c 6d 54 08 88 b8 ec c2 36 79 e9 1d 99 af f6 01 0d*
- *Valid from July 29th 2015 to December 31th 2030*
- *Key type: RSA 2048 bits – SHA256*
- *Technical constrains (*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)*
  - *Smartcard logon (1.3.6.1.4.1.311.20.2.2)*

1.3.2.4 Subordinate Certificate Authorities to other CSPs

Under the Firmaprofesional Certification Hierarchy there are several Subordinate CAs issued on behalf of other entities. These other entities must act as Certification Services Providers and they must define their own Certification Practices Statement (CPS). Firmaprofesional guarantee to these certificates the same level of technical security that the public certificates, as they are operated from the same infrastructure and from the same facilities.

Currently Firmaprofesional Certification Hierarchy hosts 3 CAs for other Certification Services Providers.

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

[5] Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates. CA/Browser Forum. Version 1.3.0 April 16, 2015
[6] Mozilla CA Certificate Inclusion Policy. Version 2.2

There are two versions of this certificate with the same RSA 4096 bits key pair and the same identification data, one generated with the algorithm SHA1 and other with the algorithm SHA256. The second one is technically constrained through the use of the *Extended Key Usage* (EKU – *extKeyUsage*) extension, pursuant Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates[7] and Mozilla CA Certificate Inclusion Policy[8].

- ***CN=SIGNE Autoridad de Certificacion***
- *Hash SHA1: d730 47f2 cce5 64ef b0bc 8568 93ea 19d7 7469 398c*
- *Hash MD5: 836D 31CF CB46 C6E0 3639 9E08 4D9D 47BB*
- *Valid from 21 July 2010 to 21 July 2022*
- *Key Type: RSA 2048 bits – SHA1*
- CPS: *https://www.signe.es/signe-ac/dpc*

- ***CN=SIGNE Autoridad de Certificacion***
- *Hash SHA1: e6 b5 2b 5d 52 e5 cd e9 86 2a c1 de 66 8e c9 53 ad 36 59 bd*
- *Valid from July 29th 2015 to December 31th 2030*
- *Key type: RSA 2048 bits – SHA256*
- *Technical constrains (*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)*
  - *Smartcard logon (1.3.6.1.4.1.311.20.2.2)*
- *CPS: https://www.signe.es/signe-ac/dpc*

SEU (Servicios Electrónicos Universitarios / Electronic University Services) is a Colombian company focused on serving colleges and universities in Colombia in the field of eGovernment.

There are two versions of this certificate with the same RSA 4096 bits key pair and the same identification data, one generated with the algorithm SHA1 and other with the algorithm SHA256. The second one is technically constrained through the use of the *Extended Key Usage* (EKU – *extKeyUsage*) extension, pursuant Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates[9] and Mozilla CA Certificate

[7] Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates. CA/Browser Forum. Version 1.3.0 April 16, 2015
[8] Mozilla CA Certificate Inclusion Policy. Version 2.2
[9] Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates. CA/Browser Forum. Version 1.3.0 April 16, 2015

Inclusion Policy[10].

- ***CN=SEU Autoridad de Certificacion***
- *Hash SHA1: 432C 2A08 ED3E 4ACB 87E8 4704 DCFD 9C3B D84D 18B7*
- *Hash MD5: 7F42 E95B FA34 A8D5 DFEA BA25 139F 9C81*
- *Valid from 20 February 2013 to 31 December 2030*
- *Tipo de clave: RSA 2048 bits – SHA1*
- *CPS:* http://www.seu.com.co/dpc

- ***CN=SEU Autoridad de Certificacion***
- *Hash SHA1: a9 e5 52 45 74 a8 ec 1f d3 16 18 54 c9 13 4c 47 97 de 7b 09*
- *Valid from July 29th 2015 to December 31th 2030*
- *Key type: RSA 2048 bits – SHA256*
- *Technical constrains (*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)*
  - *Smartcard logon (1.3.6.1.4.1.311.20.2.2)*
- *CPS: http://www.seu.com.co/dpc*

Banco Santander offers its electronic certification services in the university environment by issuing the University Student Card (TUI).

There are two versions of this certificate with the same RSA 4096 bits key pair and the same identification data, one generated with the algorithm SHA1 and other with the algorithm SHA256. The second one is technically constrained through the use of the *Extended Key Usage* (EKU – *extKeyUsage*) extension, pursuant Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates[11] and Mozilla CA Certificate Inclusion Policy[12].

- ***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 26 May 2012 to 31 December 2030*
- *Key Type: RSA 2048 bits – SHA1*
- *CPS:* http://www.tuisantander.com/cps

[10] Mozilla CA Certificate Inclusion Policy. Version 2.2
[11] Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates. CA/Browser Forum. Version 1.3.0 April 16, 2015
[12] Mozilla CA Certificate Inclusion Policy. Version 2.2

- ***CN=Santander Digital Signature***
- *Hash SHA1: b0 0c 00 03 4b 72 3f 4d 95 37 35 3c 82 93 a9 45 51 4d ab 2d*
- *Valid from July 29th 2015 to December 31th 2030*
- *Key type: RSA 2048 bits – SHA256*
- *Technical constrains (*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)*
  - *Smartcard logon (1.3.6.1.4.1.311.20.2.2)*
- *CPS: http://www.seu.com.co/dpc*

1.3.2.5 Expired Certificate Authorities

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

- ***CN = Autoridad de Certificacion 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 25 October 2001 to 25 October 2013*
- *RSA key length 2048 bits*

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

This Subordinate CA was renewed with the same private key and the same name. This certification model with shared keys is called "Cross-Certification[13]". As a result, the end-user certificates issued to date may be validated both with the hierarchy based on the CA that expires in 2013 and with the hierarchy based on the CA that expires in 2030.

Firmaprofesional Subordinate CA Certificate, expired in 2013, has the following identification data:

[1] "Cross-Certification" is a mechanism which enables the creation of multiple certification paths. In this case it means that the same certificate can be validated equally in two certification hierarchies under distinct Root CAs. (See "RFC4949: Internet Security Glossary, Version 2": cross-certification).

- ***CN = AC Firmaprofesional - CA1***
- *Hash SHA1: 037C F211 8F13 EAA6 121E B035 6F9B 601C 9295 338E*
- *Hash MD5: 35D8 35EC AF1C AF08 7DD5 8727 8AB2 0B19*
- *Valid from 27 March 2003 to 26 March 2013*
- *RSA key length 2048 bits*

1.3.3 Registration Authority (RA)

A Registration Authority (RA) of Firmaprofesional is the entity responsible for:

- Processing applications for certificates.
- Identifying the applicant and verifying compliance with the requirements necessary for the certificate application.
- Validating the personal circumstances of the person who will be the certificate's signer.
- Managing the generation of key-pairs and the issuance of the certificate
- Presenting the certificate to the subscriber.

The following may act as RA of Firmaprofesional:

- Any Corporation which is a client of Firmaprofesional, issuing certificates in the name of the corporation or to the members of the corporation.
- Any trusted institution reaching an agreement with Firmaprofesional, acting as an intermediary on behalf of Firmaprofesional.
- Firmaprofesional itself directly.

Firmaprofesional shall contractually formalize the relations between itself and each of the entities that act as an RA of Firmaprofesional.

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

Where the geographical location of subscribers represents a logistical obstacle in identifying the subscriber and in the application for and delivery of certificates, the RA may delegate these functions to another trusted body. This entity must have a special relationship with the RA and a close relationship with the certificate subscribers to justify such delegation. The trusted party is required to sign a partnership agreement with the RA in which the

delegation of these functions is agreed. Firmaprofesional must be informed of and give express authorization to the agreement.

1.3.4 Applicant

The Applicant is the individual who, on their own behalf or on behalf 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 certificate applied for and will be set out in the "**Certificate Policy**" of each specific type of certificate.

1.3.5 Subscriber

The subscriber is the natural or legal person that has engaged Firmaprofesional certification services. The subscriber will therefore be the owner of the certificate.

In general, the subscriber of a Firmaprofesional certificate will be a corporation (private company, public entity, professional association), and the subscriber's identity will appear on the certificate itself. In this case, the subscriber may act as RA, managing the issuance of certificates on behalf of the corporation or members of the corporation.

1.3.6 Signer

The Signer is the person who holds a signature creation device and acts either on his/her own behalf or on behalf of the legal person which he/she represents.

The custody of the signature creation data associated with each electronic certificate of a legal person shall be the responsibility of the individual applicant, whose identification will be included in the electronic certificate.

1.3.7 Relying Party

The Relying Party is a third party who trusts in the certificate, and is any person or organization who voluntarily relies on a certificate issued by Firmaprofesional.

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

Firmaprofesional Root Certificates are recognized by leading software vendors such as Microsoft, Apple or Mozilla Foundation.

Firmaprofesional duties and responsibilities with respect to third parties who voluntarily trust its certificates are limited to those contained in this CPS and those laid down in Law

59/2003 on electronic signatures

Third parties who rely on these certificates should keep the limitations on their use in consideration.

1.4 Types of Certificates

1.4.1 Qualifier Corporate Certificates

Corporate Certificates are qualified certificates pursuant to Law 59/2003 on electronic signatures where the subscriber is a Corporation (a company, organization, a professional association or Government Agency):

- **Corporate Certificate for Professional Membership Organizations**: Are qualified certificates of physical persons identifying the subscriber as a Professional Association and the signer as a professional member of that Association.
- **Corporate Certificate for Legal Representatives**: These are qualified certificates of physical persons identifying the subscriber as a Corporation and the signer as legal representative of that Corporation.
- **Corporate Certificates for Legal Persons**: These are qualified certificates of legal persons pursuant to article 7 of Law 59/2003
- **Corporate Certificates for Natural Persons**: These are qualified certificates of natural persons which identify the subscriber as a Corporation and the signer as linked to the Corporation, whether as an employee, associate, partner, customer or supplier.

OID CERTIFICATE POLICIES	
1.3.6.1.4.1.13177.10.1.1.D	Corporate certificate for professional membership organizations CP
1.3.6.1.4.1.13177.10.1.2.D	Corporate certificate for natural persons CP
1.3.6.1.4.1.13177.10.1.5.D	Corporate Certificate for Legal Persons CP
1.3.6.1.4.1.13177.10.1.11.D	Corporate Certificate for Legal Representatives CP

D = Device / Security Level:
1 = SSCD (High Level), 2 = Other Devices (Intermediate Level)

1.4.2 Restricted Use Corporate Certificates

Restricted Use Corporate Certificates are electronic certificates issued under Law 59/2003 on electronic signature which Subscriber is a corporation (whether a company, an organization, a professional or a Public Administration):

- **Corporate certificate for Electronic Invoicing:** These are qualifier certificates of

natural persons with powers to represent an organization to sign Electronic Invoices.

- **Corporate Company Seal Certificates: These are e**lectronic certificates of juridic person limited for specific uses.

  The Corporate Company Seal Certificates have been approved for use in electronic invoicing and certified scanning, by authorization of the Director of the Tax Department, mechanism set out in Article 18 of Royal Decree 1496/2003, of November 28, by approving the regulation regulating invoicing requirements, and amending Regulations on Value Added Tax

OID CERTIFICATE POLICIES	
1.3.6.1.4.1.13177.10.1.6.D	Corporate Certificate for Electronic Invoicing CP
1.3.6.1.4.1.13177.10.1.10.D	Corporate Company Seal Certificates CP

D = Device / Security Level:
1 = SSCD (High Level), 2 = Other Devices (Intermediate Level)

1.4.3 Certificates for the Public Administration

Certificates for the Public Administration are electronic certificates issued in accordance with the requirements laid down by **Law 11/2007 on Citizens' Electronic Access to Public Services**.

- **Digital stamps for the Civil Service, public bodies or corporations:** These are certificates for IT devices, programs or applications enabling signatures on behalf of the body in electronic signature systems for automated administrative action.

- **Certificate of Public Employees:** These are certificates of natural persons which identify the subscriber as the Public Administration and the signer as an employee of the Administration.

OID CERTIFICATE POLICIES	
1.3.6.1.4.1.13177.10.1.21.D	Public Body Digital Stamp CP
1.3.6.1.4.1.13177.10.1.22.D	Public Employee CP

D = Device / Security Level:
1 = SSCD (High Level), 2 = Other Devices (Intermediate Level)

1.4.4 Qualified Personal Certificates

Qualified Personal Certificates are qualified certificates pursuant to Law 59/2003 on electronic signatures:

- **Qualified Personal Certificates**: Qualified Certificates of physical persons.

OID CERTIFICATE POLICIES	
1.3.6.1.4.1.13177.10.1.40.2	Personal CP

1.4.5 Secure Services Certificates

Firmaprofesional issues digital certificates for uses other than to provide electronic signatures. These certificates are not governed by Law 59/2003. The Subscriber is a Corporation (a company, organization, a professional association or a body of the Public Administration):

- **Web SSL Server Certificate:** These are Certificates are used to authenticate a Web server by browsers using the HTTPS protocol.
- **Web SSL Server Extended Validation Certificate:** These are certificates are used to authenticate a Web server by browsers using the HTTPS protocol with extended warranties validation about the entity that owns the server.
- **Electronic Office Certificate**: These are Certificates issued to public authorities to authenticate the identity of the Electronic Office (official website), according to the requirements of Law 11/2007 of Electronic Access to Public Services.
- **Code Signing Certificate:** These are certificates used to sign executable code, such as a Java applet, giving a guarantee of its authorship and integrity against unauthorized modification.
- **Infrastructure Certificate**: These are certificates are used to authenticate the identity of a server by using encrypted communication protocols such as SAML, TLS or IPSEC.
- **Secure Service Certificate (VA / TSA):** These are certificates that allow the signature of digital evidence as Time Stamping Authority (**TSA**) or Validation Authority (**VA**). Their issue and use requires the maximum guarantee of security.

OID CERTIFICATE POLICIES	
1.3.6.1.4.1.13177.10.1.3.1	SSL Web Server CP
1.3.6.1.4.1.13177.10.1.3.10	SSL EV Web Server CP
1.3.6.1.4.1.13177.10.1.20.1	Electronic Office CP
1.3.6.1.4.1.13177.10.1.30.1	Infrastructure CP
1.3.6.1.4.1.13177.10.1.8.1	Code Signing CP

1.3.6.1.4.1.13177.10.1.4.1	Secure Service CP (TSA / VA)

1.4.6 Advanced Digital Signature Certificates

Private Certificates are not qualified certificates under the terms of the Spanish Electronic Signature Law. The characteristics of these certificates are defined with respect to each Subscriber and they are for private use according to the Subscriber's setting.

Certificates issued by Firmaprofesional which do not have a policy explicitly mentioned in this CPS or which have no specific policy should be interpreted as being certificates issued for private use.

These certificates are for private use and are not issued with qualification; as such, there is no requirement to publish their certification policies and practices, and their inclusion in the present CPS is voluntary.

1.5 Unauthorized use of certificates

Any use is prohibited which is contrary to Spanish and EU regulations, contrary to international conventions ratified by the Spanish government, or which contravenes generally accepted good habits, practices or public order. Any use other than as provided in this Certification Practice Statement (CPS) and its corresponding Certificate Policy is also prohibited.

Certificates are not designed for use or resale as control devices in hazardous situations or for uses requiring failsafe performance such as in the operation of nuclear facilities, aerial navigation or communications systems, or weapons control systems, where failure could lead directly to death, personal injury or severe environmental damage, and any such use, or resale for such use, is not authorized.

The end-user certificates cannot be used to sign public key certificates of any kind, nor can they be used to sign certificate revocation lists.

Firmaprofesional not store copies of Subscriber private keys, not being able to recover data encrypted with the corresponding public key in case of loss or mutilation of the private key or device that custody by the Subscriber. Subscribers who decide to encrypt information do so entirely at their sole and own responsibility. Firmaprofesional shall accept no liability whatsoever for loss of information resulting from the loss of encryption keys. As such, Firmaprofesional does not recommend the use of digital certificates for the encryption of information.

1.6 Policy Management

1.6.1 Responsible organization

Firmaprofesional Technical Department is responsible for the management of this CPS and of the Certificate Policies.

1.6.2 Contact person

Organization responsible :	Firmaprofesional, S.A.
Contact person:	Firmaprofesional Technical Director
E-mail:	info@firmaprofesional.com
Telephone:	+34 93 477 42 45
Address:	Firmaprofesional, S.A. Edificio ESADECREAPOLIS. Avenida Torre Blanca, 57. Sant Cugat del Valles 08173 (Barcelona)

1.6.3 Frequency of review

The CPS and the various CPs shall be reviewed, and where necessary updated, on an annual basis.

1.6.4 Approval Procedure

The publication of revisions to be made to this CPS and to the Certificate Policies of each type of certificate require approval by the CEO of Firmaprofesional, after verification of the compliance of the requirements stated therein.

1.7 Definitions and acronyms

1.7.1 Definitions

- **Certification Services Provider**: natural or legal person who issues electronic certificates or provides other services related to electronic signatures.
- **Electronic Certificate**: A document signed electronically by a certification services provider which links signature verification data to a signer and confirms their identity.
- **Qualified Certificate**: Certificate issued by a Certification Services Provider that meets the requirements established in law in terms of providing verification of the identity and other circumstances of the applicants and in terms of the reliability and the guarantees of the certification services provided, in accordance with the provisions of Chapter II of Title II of Law 59/2003 of 19 December on electronic signatures.
- **Public Key and Private Key:** the asymmetric cryptography on which PKI is based; its uses a pair of keys where the content encrypted on one key can only be decrypted with the other key and vice versa. One of these keys, called the public key, is included in the electronic certificate, while the other, called the private key, is known only to the certificate holder.
- **Signature Creation Data (Private Key):** unique data, such as codes or private cryptographic keys, which the signer uses to create the electronic signature.
- **Signature Verification Data (Public Key):** data, such as codes or public cryptographic keys, which are used for the purpose of verifying the electronic signature.
- **Secure Signature-Creation Device (SSCD)**: Device which is used to apply the Signature creation data and which complies with the requirements of Article 24.3 of Law 59/2003 of 19 December on electronic signatures (usually a smart card).
- **Electronic Signature**: data in electronic form which are attached to or associated with other data and which serve as a means of personal identification.
- **Advanced Electronic Signature**: electronic signature which allows the personal identification of the signer to be established in respect of the signed data and provides verification of its integrity; it is uniquely linked the signer and the data it refers to, and it is created using means that the signer can maintain under his/her sole control.

- **Qualified Electronic Signature**: advanced electronic signature which is based on a qualified certificate and created by a secure signature-creation device.
- **Hash Function**: is an operation that is performed on a dataset of any size, so that the result obtained is another dataset whose size is fixed, regardless of the original dataset's size, and which has the property of being unequivocally associated to the initial data.
- **Certificate Revocation Lists (CRL)**: lists containing the details of revoked or suspended license.
- **Hardware Security Module (HSM)**: Hardware module used to perform cryptographic functions and store keys in a secure manner.
- **Time stamp**: is a special type of electronic signature, issued by a trusted third party, which guarantees the integrity of a document at a determined date and time.
- **Time Stamping Authority (TSA)**: Trusted entity that issues timestamps.
- **Validation Authority (VA)**: Trusted entity that provides information on the validity of digital certificates and electronic signatures.

1.7.2 Acronyms

CA: Certification Authority

CA Sub: Subordinate Certification Authority

CP: Certificate Policy

CPS: Certificate Practice Statement

CRL: Certificate Revocation List

HSM: Hardware Security Module

LDAP: Lightweight Directory Access Protocol

OCSP: Online Certificate Status Protocol.

OID: Object identifier

PKI: Public Key Infrastructure

CSP: Certification Services Provider

RA: Registration Authority

TSA: Time Stamp Authority

VA Validation Authority

Standards and Standardization Bodies

CEN: European Committee for Standardization

CWA: CEN Workshop Agreement

ETSI: European Telecommunications Standard Institute

FIPS: Federal Information Processing Standard

IETF: Internet Engineer Task Force

PKIX: PKI Working Group of the IETF

PKCS: Public Key Cryptography Standards

RFC: Request For Comments

2 REPOSITORIES AND PUBLICATION OF INFORMATION

2.1 Repositories

Access	Description	URL
Public	CPS y Certificate Policies	http://www.firmaprofesional.com/cps
Public	CA Root SHA1	http://crl.firmaprofesional.com/caroot.crt
Public	CA Root SHA256	http://crl.firmaprofesional.com/caroot256.crt
Public	CRL Root CA	http://crl.firmaprofesional.com/fproot.crl
Public	Subordinate CA CA1	http://crl.firmaprofesional.com/ca1.crt
Public	CRL Subordinate CA CA1	http://crl.firmaprofesional.com/firmaprofesional1.crl
Public	Subordinate CA AAPP	http://crl.firmaprofesional.com/fpaapp.crt
Public	CRL Subordinate CA AAPP	http://crl.firmaprofesional.com/fpaapp.crl
Public	Subordinate CA CUALIFICADOS	http://crl.firmaprofesional.com/cualificados.crt
Public	CRL de CA Sub CUALIFICADOS	http://crl.firmaprofesional.com/cualificados.crl
Public	Subordinate CA INFRAESTRUCTURA	http://crl.firmaprofesional.com/infraestructura.crt
Public	CRL CA Sub INFRAESTRUCTURA	http://crl.firmaprofesional.com/infraestructura.crl
Public	Subordinate CA CFEA	http://crl.firmaprofesional.com/cfea.crt
Public	CRL Subordinate CA CFEA	http://crl.firmaprofesional.com/cfea.crl
Public	Subordinate CA OTC	http://crl.firmaprofesional.com/otc.crt
Public	CRL Subordinate CA OTC	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 their URL. Any change in the URLs is notified to all potentially affected parties.

The IP addresses corresponding to each URL may be multiple and dynamic, and are subject to change without notice.

2.2 Publication of information

2.2.1 Certification Policies and Practices

Both the current CPS and the Certificate Policies of each type of certificate will be available in electronic format on Firmaprofesional website.

Earlier versions will no longer be available for on-line consultation, but may be obtain on request by contacting Firmaprofesional.

2.2.2 Terms and conditions

The contractual relationship between Firmaprofesional and its Subscribers is based on the signing of a ***Contract for the Provision of Certification Services*** and acceptance of *Firmaprofesional* ***General Terms and Conditions***, as published on its website at http://www.firmaprofesional.com/cps

2.2.3 Dissemination of the certificates

The Certificate Subscriber is responsible for ensuring that their certificates are obtainable by any third party who wishes to authenticate a user or verify the validity of a signature. This is usually achieved automatically by attaching the certificate to an electronically signed document.

Firmaprofesional is not obliged to publish the issued certificates in a publicly accessible repository. However, in order to improve services to its clients, Firmaprofesional is able to offer Directory, search and download services for some certificates issued under its certification hierarchy.

2.3 Frequency of publication

The Root CA will issue a **List of Revoked CAs (ARL)** at least every six months, or exceptionally, when there is revocation of an authority certificate.

Each Subordinate CA will issue a **Certificate Revocation List (CRL)** on a daily basis, and exceptionally, whenever a certificate is suspended or revoked.

Firmaprofesional shall publish any change in its certification policies and practices with immediate effect.

2.4 Control of access to repositories

The CPS, the Certificate Policies, the General Conditions, the CA certificates and certificate revocation lists (CRL) are published in publicly accessible repositories not subject to

controlled access.

Issued Certificates may be published in public repositories or in restricted access repositories as required. Validation services by OCSP protocol and time stamping by TSP protocol are services subject to restricted access and payment.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Registration of Names

3.1.1 Types of names

All certificates require a distinguished name (DN) according to the X.500 standard. Additionally, all the names on qualified certificates shall be consistent with the stipulation of the following standards:

- ETSI TS 101 862 known as "European profile for Qualified Certificates"
- RFC 3280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile",
- RFC 3739 "Qualified Certificates Profile".

3.1.2 Need for names to be meaningful

DN fields relating to Given Names and Surnames shall correspond to the signer's legally registered data and shall be expressed exactly in the format that appears on the national identity card, residence card, passport or other document recognized in law.

Where the information contained in the DN is fictitious or where its invalidity is expressly stated (e.g. "TEST" or "INVALID"), the certificate shall be rendered legally invalid, and shall be valid only for the purposes of technical interoperability testing.

3.1.3 Use of pseudonyms

The certificates do not allow, in any situation, the use of a signer’s pseudonyms.

3.1.4 Rules for interpreting different formats of names

In all cases Firmaprofesional observes the stipulations of the X.500 standard referenced 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 signer. The CIF or NIF (tax identification number) attribute is used to distinguish between two identities when there is a problem of duplicated names.

3.1.6 Recognition, authentication and role of trademarks

The CA assumes no commitments in the issuance of certificates in respect of the use by subscribers of a trademark. Firmaprofesional deliberately prohibits the use of a name whose right of use is not the property of the subscriber. However, the CA is not required to seek evidence of trademark ownership prior to issuing certificates.

3.2 Initial validation of identity

3.2.1 Method to prove possession of the private key

When issuing a certificate on a hardware device, the private key is created in the moment immediately preceding certificate generation, in a procedure which ensures confidentiality and its link to the applicant's identity.

Each RA is responsible for ensuring secure delivery of the applicant's device.

In other cases, proof of the subscriber's possession of the private key is achieved through the delivery of PKCS#10 or equivalent cryptographic proof or other method approved by Firmaprofesional.

3.2.2 Authentication of the identity of a legal person

The Registration Authority shall verify the following information to enable authentication of the organization's identity:

- Data relating to the name or business name the organization.
- Data relating to the constitution and legal status of the subscriber.
- Data on the extent and validity of the applicant's powers of representation.
- Data regarding the tax identification code of the organization or equivalent code as used in the country to whose law the subscriber is subject.

Firmaprofesional reserves the right not to issue a certificate in the event that it considers that the documentation provided is insufficient or inappropriate for the purpose of verifying the data set out above.

3.2.3 Authentication of the identity of a natural person

The RA shall reliably verify the identity of the person identified in the certificate. As such, the natural person **should present themselves** and present their National Identity Document, residency card, passport or other means of identification which is recognized in law.

In the event that the subscriber seeks modification of the personal identification data to be registered in respect of the identification document presented, he/she shall be required to present the Civil Registration Certificate where the variation is recorded.

The RA will verify, through the presentation of sufficient original documentation and by means of its own sources of information, the remaining data and attributes to be included in the certificate (distinguished name of the certificate), and is required to retain the documentation supporting the validity of such data as it is unable to prove using its own data sources.

Application of the provisions of the preceding paragraphs may not be required with respect to certificates issued subsequent to 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 the certificate applicants has already been obtained by the RA as a result of a pre-existing relationship, in which, for the identification of the applicant, the steps stipulated in the first paragraph have been concluded and the time period elapsed since the performance of said identification is not more than five years.

b) When, in applying for a certificate, use is made of another certificate which was issued pursuant to the identification of the signer in accordance with the procedures set out in the first paragraph and where the RA is satisfied that the period of time elapsed since the verification of identification is not more than five years.

3.2.4 Authentication of the identity of the RA and the RA's operators

In the constitution of a **new RA**, the following actions shall be undertaken:

- Firmaprofesional shall verify the existence of the entity using its own sources of information.
- An authorized representative of the organization shall be required to sign a contract with Firmaprofesional, which contract shall set out the specific aspects of the delegation and the responsibilities of each party.

Furthermore, and with respect to the **RA's operators,** the RA shall be bound to:

- Verify and validate the identity of the RA's new operators. The RA shall send documentation to Firmaprofesional corresponding to the new operator and his/her authorisation to act as an operator of the RA.
- Ensure that the RA operators have received adequate training to perform their

duties, attending at least one operator training session.

- Ensure that communication between the RA and Firmaprofesional is conducted securely using operator digital certificates.

3.2.5 Domain Validation

To guarantee that an applicant entity has control over the domain (URL) which it seeks to include in a certificate, two types of checks are performed:

- **Organizational checks**: the ownership title of the domain name is requested and is certified by a legal representative of the organization.
- **Technical checks**: the following authenticated WHOIS services are consulted:
    - For "*.es" domains: https://www.nic.es/sgnd/dominio/publicInformacionDominios.action
    - For all other domains: https://www.networksolutions.com/whois/index.jsp

3.2.6 Email validation

In general, the signers are people linked to the Registration Authority (for example, associates, association members, etc.). In these cases it is not the signer who requests a specific email address to be included in the certificate but the RA itself which, by consulting its database, obtains the address.

In cases where the signer has no connection with the RA, verification of the e-mail address is performed using a challenge-response mechanism

3.3 Identification and authentication upon certificate renewal

3.3.1 Renewal of certificates online

Subscribers are able to identify and authenticate themselves in the online renewal process by using a qualified certificate, provided that the following conditions are fulfilled:

- The RA has authorized the renewal.
- The certificate to be renewed has not expired.
- In the case of qualified certificates, when a period of not more than 5 years has

elapsed since their last appearance and identification before the RA[14].

Specific requirements may differ depending on the type of certificate applied for and will be set out in the corresponding "**Certificate Policy**".

3.3.2 Renewal of certificates conducted in person

The identification process shall be conducted in the same way as when issuing a new certificate.

3.4 Identification and authentication in certificate revocation

The identification of the signers in processes of certificate revocation may be carried out by:

a) **The signer herself**: Identifying and authenticating themselves using the Revocation Code on Firmaprofesional website.

b) **Any Firmaprofesional RA:** which shall identify the signer in respect of a revocation request, according to the specific means it deems necessary.

[14] According to Article 13, paragraph 4b) of the Law 59/2003 of 19 December on electronic signatures

4 OPERATIONAL REQUIREMENTS FOR THE LIFE CYCLE OF CERTIFICATES

4.1 Certificate Requests

4.1.1 Who can apply for a certificate

The requirements to be met by an applicant depend on the type of certificate they are applying for and are set out in the "**Certificate Policy**" applicable to each specific type of certificate.

4.1.2 Certificate Application Procedures

The applicant should contact Firmaprofesional or one of its Intermediaries which acts as RA in order to manage the certificate application.

The RA will provide the applicant with the following information[15]:

- The documents which have to be submitted in order to process the application and to verify the signer's identity.
- Its availability to perform the registration process.
- Information on the issuing and revocation process, procedures governing custody of the private key and the responsibilities and conditions of use of the certificate and the device.
- Information on how the present document and the certificate policies can be accessed and consulted.

The documentation required when applying for each type of certificate is specified in the Certificate Policies (CP).

Where the applicant is a corporation acting as a Firmaprofesional RA, the Corporation may manage the applications directly accessing Firmaprofesional computer systems and generating the corresponding certificates for the Corporation itself or for its members.

[15] According to article 18 b) of Law 59/2003 of 19 December on electronic signatures.

4.2 Processing of certificate applications

4.2.1 Performing the identification and authentication functions

The RA is responsible for performing the identification and authentication of the signer in a reliable manner. This process should be concluded prior to issuing the certificate.

4.2.2 Approval or denial of certificate applications

Once the application for a certificate has been made, the RA shall verify the information provided by the applicant, including the validity of signer's identity.

If the information is found to be inaccurate or false, the RA will deny the application and inform the applicant as to the reasons for said denial. If the information is correct, the legal instrument shall be signed, which shall be binding between the subscriber and/or applicant and Firmaprofesional.

The certificate will then be issued.

4.3 Issue of certificates

4.3.1 Actions taken by CA during the issue of certificates

For the issuance of certificates shall take the following actions:

- To generate a key pair in a safe manner, ensuring the signer the exclusive access to the signature creation data.
- If necessary, the RA will deliver to the signer the necessary mechanisms to make use of the signature creation data (eg, physical delivery of the SSCD, activation codes, etc. ...)
- If necessary, the signer will deliver its public key to the RA.
- The RA will check again the content of the certificate request with the submission. If the verification is successful, the RA will validate the request.
- The RA will send to the CA the signer's public key with the verified data through a secure channel.
- The CA will verify the origin and integrity of the data sent by the RA.
- If everything is correct, the CA will issue the certificate using a procedure that ensure the confidentiality of the data exchanged and not allow falsification.
- During the generation of the certificates, the CA is responsible for adding the

remaining information set necessary to meet the technical and legal requirements established.

- In cases where Firmaprofesional have assurance that the device where the key pair was generated is a SSCD, the certificate will be issued with the appropriate OID.
- The certificate generated will be sent to the RA, and the RA will deliver it to the signer.

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

The CA will notify the subscriber or signer when the certificate is issued and, where necessary, inform the subscriber regarding its method of download.

4.4 Certificate Acceptance

4.4.1 How the certificate is accepted

The certificate will be accepted upon signature of the legally binding instrument made between the Subscriber and Firmaprofesional and when the certificate has been delivered, either personally or electronically.

As evidence of its acceptance, an acceptance sheet needs to be signed by the signer. The certificate shall be valid from the date of the signed acceptance sheet.

4.4.2 Publication of the certificate

Once the certificate is generated and accepted by the subscriber or signer, the certificate may be published in the certificate repositories as deemed necessary.

4.5 Using the keys and the certificate

4.5.1 Use of the private key and certificate by the subscriber

Certificates may be used in accordance with the stipulations set forth in this CPS and in the relevant Certificate Policy.

The *Key Usage* extension may be used to establish technical limits applicable to the use of the private key of the corresponding certificate. The application of these limits will depend largely on their correct implementation by third-party IT applications, whereby its regulation is beyond the scope of this document.

4.5.2 Use of the public key and of the certificate by the third parties who rely on the certificates

Third parties who rely on the certificate may use the certificates as set out in the present

CPS and the corresponding Certificate Policy.

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

4.6 Renewal of certificates without changing keys

This option is not available.

4.7 Renewal with change of keys

There are two ways of renewing certificates:

a) **In-person renewal process,** which is conducted in the same way as the procedures applied when issuing a new certificate.

b) **Online renewal process,** which is detailed below:

4.7.1 Circumstances for online renewal

Online renewal of certificates is only available where the following conditions are met:

- The RA provides an online renewal service.
- The certificate has not expired.
- In the case of qualified certificates, no more than 5 years have elapsed since the applicant's last physical presentation and identification before the RA[16].

4.7.2 Who can apply for the online renewal of a certificate

Any signer may request renewal of their certificate online provided that the circumstances described in the previous paragraph are fulfilled.

4.7.3 Online renewal application

The subscriber may contact the RA that issued their certificate and request its renewal. The RA will inform the applicant as to how to formalize their request.

4.7.4 Processing online renewal requests

The following steps will be performed:

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

- The RA will receive a notification that a certificate is about to expire. At that time, the RA may authorise its renewal.
- The signer will be notified by email that their certificate can be renewed.
- The signer will connect to Firmaprofesional website and using their certificate, sign the renewal of their certificate.
- A new pair of keys will then be generated.
- The public key will be sent to the CA through a secure channel in PKCS10 format or equivalent.
- The certificate will then be generated following a procedure that employs protection against falsification and which safeguards the confidentiality of the data exchanged.
- The certificate generated will be delivered to the subscriber.

4.7.5 Notification of the issuance of the renewed certificate

The CA will notify the subscriber and the signer that the certificate has been renewed upon successful completion of the process.

4.7.6 Form of acceptance of the renewed certificate

The certificate will be accepted through electronic signature of the renewal.

4.7.7 Publication of the Renewed certificate

Once the certificate has been renewed, the new certificate may be published in the certificate repositories as deemed necessary, replacing the previous certificate.

4.8 Modification of certificates

If modification of any data is required, the RA shall proceed with the certificate's revocation and issue a new certificate.

4.9 Certificate revocation and suspension

The revocation of a certificate implies the loss of its validity, and is irreversible.

Suspension[17] implies the temporary loss of validity of a certificate, and is reversible.

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

4.9.1 Causes for revocation

A certificate may be revoked on following grounds:

a) Circumstances which affect the information contained in the certificate:

- Alteration to any of the information contained in the certificate.
- Discovery that any of the information contained in the certificate application is inaccurate.
- Discontinuation of the signer's membership status in the case of Corporate certificate for professional membership organizations.
- Discontinuation or change in signer's relationship with the Corporation.

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

- Compromise of the private key or of the infrastructure of the CA's systems, whenever this affects the reliability of certificates issued.
- Infringement, by the CA or RA, of the requirements set forth in the certificate management procedures, as established in the CPS.
- Compromise or suspected compromise of the security of the key or of the subscriber's certificate.
- Unauthorized access or use, by a third party, of the subscriber's private key.
- Improper use of the certificate by the subscriber or signer.

c) Circumstances affecting the security of the cryptographic device:

- Compromise or suspected compromise of the security of the cryptographic device.
- Loss or disablement due to damage of the cryptographic device.

[17] Suspended certificates appear in the CRL with the reason for revocation “Certificate Hold (6)" (RFC 3280). In certain applications of the Microsoft Windows operating system, upon consultation of a list of revoked certificates, this cause appears translated as "Posesión de certificado (6)", which may mislead the user.

- Unauthorized access, by a third party, to the subscriber's activation data.

d) Circumstances affecting the subscriber or signer:

- Non-compliance by the subscriber or signer of the certificate with the rules governing usage as set out in this CPS or in the legally binding instrument made between Firmaprofesional and the subscriber.
- Termination of the legal relationship between Firmaprofesional and the Subscriber.
- Modification or termination of the underlying legal relationship or cause which gave basis to the certificate's issue to the signer, including temporary professional disqualification.
- Violation by the certificate applicant of the pre-established requirements governing the application.
- Violation by the subscriber of the obligations, responsibilities and guarantees established in the corresponding legal instrument or in the CPS.
- Total or partial unforeseeable incapacity.
- The death of the subscriber or signer.

e) Other Circumstances:

- The suspension of the digital certificate for a period exceeding that established in the CPS
- By court or administrative order.
- Due to the occurrence of any other reason specified in the CPS

4.9.2 Who can request revocation

The revocation of a certificate may be requested by:

- The signer who is bound to request the certificate's revocation where he/she becomes aware of any of the circumstances detailed above.
- Any person may request revocation of a certificate where they have knowledge of any of the circumstances detailed above.

The revocation of the certificate may be processed by:

- Authorized operators of the Subscriber RA.
- Authorized operators of the CA.

4.9.3 Procedures for revocation requests

There are different alternatives for the subscriber when requesting revocation of the certificate.

In any case, when suspending or revoking the certificate, notification will be sent to the subscriber, communicating the respective time and cause.

4.9.3.1 Online Procedure

Firmaprofesional will make an online from available to the subscriber which can be used to request the revocation of his/her certificate.

For this purpose, the subscriber must:

- Access the revocation section on Firmaprofesional website.
- Complete the form provided with their correct identification information.
- 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 procedure is accepted, the certificate will be immediately revoked.

The RA will receive an email from the system with notification of the certificate's revocation.

4.9.3.2 Revocation during office hours

The subscriber or the signer must contact their RA, and the RA will, in turn, identify and authenticate their identity through the procedures it considers appropriate.

Once properly identified, the operator shall complete the revocation.

4.9.3.3 Revocation outside office hours

To request revocation of a certificate by telephone outside office hours, Firmaprofesional telephone revocation service should be contacted on the following number:

Revocation Service 24x7: 902 361 639

As a preventive measure, Firmaprofesional will suspend the certificate and send a message to the RA with the suspension data and the reason.

The RA will have 15 days to verify the accuracy of the revocation request and shall accordingly complete or otherwise terminate the certificate revocation process.

If after this period, the certificate remains suspended, Firmaprofesional will proceed with its automatic revocation.

4.9.4 Period in which the CA is bound to resolve the revocation request

Once the identity of the subscriber has been authenticated as described above, and the revocation duly processed by the RA, the revocation will become immediately effective.

4.9.5 Obligation to verify revocations by third parties

Verification of the status of the certificates must be performed for each use of the certificates, by querying the Certificate Revocation List (CRL) or the OCSP service.

4.9.6 Frequency of CRL issuance

The CRL of end-entity certificates is issued at least every 24 hours, or whenever a revocation is effected, with a validity of 7 days.

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

4.9.7 Maximum time between the generation and publication of CRLs

Since the CRL is published at the time of its creation, no time is considered as elapsing between its creation and publication.

4.9.8 Availability of the online certificate status verification system

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

In case of system failure, or other factors beyond the control of the CA, the CA shall make every effort to ensure that this information service is not unavailable for more than the maximum period of 24 hours.

4.9.9 Requirements for checking revocation online

With respect to the use of the CRL service, which is an open access service, the following should be considered:

- In all cases the latest issued CRL should be checked, which can be downloaded from the URL contained on the certificate itself in the "*CRL Distribution Point*" extension.
- The user must additionally check the relevant CRL(s) of the certificate chain of the hierarchy.
- The user must ensure that the revocation list is signed by the authority that issued the certificate which it seeks to validate.
- Revoked certificates which expire will be removed from the CRL.

4.9.10 Grounds for suspension

Firmaprofesional may suspend a certificate in the following cases:

- Where it suspects that a key has been compromised, until such time as this can be confirmed or denied.
- Where the subscriber has outstanding payments due in respect of their certificate.
- Where it does not have all the information necessary to determine the revocation of a certificate.

4.9.11 Who can request suspension

Certificates may only be suspended by:

- Authorized operators of the Subscriber RA.
- Authorized operators of the CA

4.9.12 Limits of the period of suspension

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

4.10 Certificate status information services

4.10.1 Operating Characteristics

Firmaprofesional publishes Certificate Revocation Lists (CRL) on its website, as a free-of-charge service with unrestricted access.

Additionally, Firmaprofesional offers commercial certificate validation services using OCSP protocol (Online Certificate Status Protocol) or using Webservices

4.10.2 Service Availability

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

In case of system failure, or other factors beyond the control of the CA, the CA shall make every effort to ensure that this information service is not unavailable for more than the maximum period of 24 hours.

4.10.3 Additional Features

The use of OCSP services is not public and requires specific licensing.

4.11 Termination of the subscription

The subscription will terminate upon its expiration or upon revocation of the certificate.

4.12 key custody and recovery

Firmaprofesional not custody backup copies of the private keys of subscribers nor provide key scrow services.

5 PHYSICAL SECURITY, PREMISES, MANAGEMENT AND OPERATIONAL CONTROLS

5.1 Physical Controls

The CA has physical and environmental security controls in place to protect the resources of the premises where the systems and equipment used for the operations are housed.

The certificate generation services are governed by a physical and environmental security policy which offers protection against:

- Unauthorized physical access
- Natural disasters
- Fire
- Failure of support systems (electrical power, telecommunications, etc.).
- Structural collapse
- Floods
- Theft
- Unauthorized removal of equipment, information, storage devices and applications associated with components used for the services of the Certification Services Provider

Facilities are equipped with preventive and corrective maintenance systems with 24 hours attendance, 365 days per year, with assistance provided within 24 hours of notification. The location of the premises guarantees the presence of law enforcement officers in a period not exceeding 30 minutes, due to its location in the centre of a provincial capital.

5.1.1 Physical location and construction

The CA's premises were constructed using materials that ensure protection against brute force attacks, and are located in an area with a low risk of disasters and which allows rapid access.

Specifically, the room where cryptographic operations are performed is a Faraday Cage with protection from external radiation, double flooring, fire detection and suppression systems,

anti-moisture systems, dual refrigeration and dual power supply system.

5.1.2 Physical Access

Physical access to the premises of the Certification Services Provider where the certification processes are performed is restricted and protected using a combination of physical and procedural measures.

Access is limited to specifically authorized personnel, with identification control and registration at point of access, including with use and archive of CCTV.

The premises are equipped with motion detectors at all vulnerable points and intrusion detection alarm systems with alerts provided via alternative channels.

Access to the rooms is controlled with identification card readers and fingerprinting, managed by a computer system that maintains an automatic log of entries and exits.

5.1.3 Power supply and air conditioning

The CA's premises have electrical surge protection equipment and a backup electrical supply system using back up equipment and a redundant generator with fuel tanks which can be refilled from the outside.

The rooms housing computer equipment are equipped with temperature control systems with backup air conditioning equipment.

5.1.4 Exposure to water

The rooms housing computer equipment have a moisture detection system.

5.1.5 Fire Protection and Prevention

The rooms housing computer equipment are installed with automatic fire detection and extinction systems.

5.1.6 Storage System

Each removable storage system (tapes, cartridges, diskettes, etc.) which contains confidential information is marked with the highest level confidentiality classification of the information it contains, and can only be accessed by authorized personnel.

Information classified as *Confidential*, regardless of the storage device used, is stored in fireproof or permanently locked cabinets, with express authorization required before removal.

5.1.7 Elimination of data storage devices

When no longer useful, sensitive information is destroyed using the most suitable method according to the device used to store the information:

- Print and paper, using paper shredders or special waste paper bins for later supervised destruction.
- Storage devices: before being discarded or reused, these will be wiped, physically destroyed or the information made unreadable.

5.1.8 Backup copies stored offsite

The CA maintains a secure external storage site for the custody of documents and of magnetic and electronic devices which is separate from the operations centre.

Two expressly authorized persons are required to access, deposit or remove devices.

5.2 Procedural controls

5.2.1 Roles of responsibility

Trusted roles are described in the respective Certificate Policies of the hierarchy so as to ensure a segregation of functions that provide control and limit the possibility of internal fraud, whereby no single person is granted control of all certificate functions from start to finish.

As specified in the standard CEN CWA 14167-1, the minimum established roles are:

- Security Officer: Has overall responsibility for the administration and implementation of security policies and procedures
- System Administrators: Authorized to make changes to the system's configuration, but has no access to its data.
- System Operator: Responsible for the day-to-day management of the system (monitoring, backup, recovery,…)
- System Auditor: Authorized to access the system logs and verify the procedures that are performed on the system.
- CA Operator - Certificate Operator: Responsible for activating the keys of the CA in the online environment, or for certificate signing and CRL processes in the Offline Root environment.

- Registration Officer: Responsible for approving, issuing, suspending and revoking End-entity certificates.

5.2.2 Number of persons required per task

The CA guarantees at least two people to perform tasks that require *multi-person control* and as detailed below:

- The generation of the key of the CAs.
- The recovery and back-up of the private key of the CAs.
- The issue of CA certificates.
- Activation of the private key of the CAs.
- Any activity performed on hardware and software resources that support the root CA.

5.2.3 Role-based identification and authentication

The individuals assigned to each role are identified by the system auditor, ensuring that each staff member performs the operations to which they are assigned.

Each staff member controls only the resources necessary for their role, ensuring that no person is able to gain access to unallocated resources.

Access to resources is performed, depending on the asset, by means of login/password, digital certificates, physical access cards and keys.

5.2.4 Roles requiring separation of duties

The tasks of the auditor are inconsistent in time with the tasks of Certification and incompatible with Systems. These functions are subordinate to the head of operations, reporting both to him/her and to the technical manager.

Staff involved in Systems Administration may not engage in any activity involving Auditing or Certification tasks.

5.3 Personnel controls

5.3.1 Requirements with respect to qualifications, knowledge and professional experience

All personnel performing tasks deemed as trusted without supervision have at least six months working in the production centre and have fixed employment contracts.

All staff is qualified and is properly trained to perform the operations that have been assigned to them.

The CA will ensure that record staff is personnel from a Corporation trusted to perform registration tasks. To this effect a declaration is required to that effect from the Entity taking on the role of RA.

Registration staff shall have completed a training course in order to carry out tasks involving the registration and validation of requests. At the end of the course, an external auditor will assess their knowledge of the process.

Firmaprofesional will remove any employee from critical functions whenever it becomes aware that any offense has been committed that may affect the performance of these functions.

5.3.2 Background check procedures

Firmaprofesional conducts relevant research before employing any person.

The RAs may establish different criteria, being responsible for the actions of those persons which they authorize.

5.3.3 Training Requirements

Firmaprofesional conducts the training necessary to ensure the proper performance of certificate tasks, especially when substantial changes are made to such tasks and according to the individual knowledge of each operator.

5.3.4 Requirements and frequency of refreshment training

Updates will be performed on an annual basis, except for amendments to the CPS, which will be notified as they are approved.

5.3.5 Sanctions in case of unauthorized actions

Firmaprofesional has an internal disciplinary system in the event of unauthorized actions which culminate with the termination of employment.

5.3.6 Requirements governing the contracting of third parties

Employees hired to perform critical tasks are required previously to sign the confidentiality clauses and be bound by the operational requirements practised by the CA. Any action that compromises the security of accepted critical processes may lead to termination of employment.

5.3.7 Documentation supplied to personnel

Firmaprofesional will make documentation available to all personnel detailing the assigned functions, policies and practices governing these processes and the respective security documentation.

Additionally, it will provide documentation required by staff at all times, in order that they may conduct their duties competently.

5.4 Security audit procedures

5.4.1 Types of registered events

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

- Switching on and off of the system.
- Attempts to create, delete or set up passwords or change privileges.
- Attempts to start and end sessions.
- Unauthorized attempts to access the CA's system through the network.
- Unauthorized attempts to access the CA's internal network.
- Unauthorized attempts to access the file system.
- Physical access to the logs.
- Changes in the system's configuration and maintenance.
- Application records of the Certification Authority.
- Switching on and off the CA's application.
- Changes to the CA's details and/or keys.
- Changes in the creation of certificate profiles.
- Own key generation.
- Life cycle events of the certificate.
- Events associated with the use of the of the CA's cryptographic module.
- Destruction records for storage devices containing the keys, activation data.

Additionally, Firmaprofesional retains, either manually or electronically, the following information:

- The creation ceremonies of CA keys and the key management databases.
- Physical access logs.
- Maintenance and changes in the system's configuration.
- Changes in personnel performing critical tasks at the CA.
- Reports of compromises and discrepancies.
- Records on the destruction of material containing key information, activation data or personal information of subscribers, where this information is managed.
- Possession of activation data, for operations with the private key of the CAs.

5.4.2 Frequency of audit log processing

The audit logs are reviewed on a weekly basis and, in any case, when a system alert is produced due to the occurrence of an incident, in search of suspicious or unusual activity.

5.4.3 Audit logs retention period

Audit log information is retained for the length of time deemed necessary to ensure the security of the system and in accordance with the actual importance of each log.

5.4.4 Protection of audit logs

The system logs are protected from manipulation by the signing of the files that contain them.

They are stored in fireproof devices.

Their availability is protected by storage in external facilities separate from the centre where the Certification Authority is located.

The devices are managed at all times by authorized personnel.

5.4.5 Audit log backup procedures

Firmaprofesional has a suitable backup procedure so that, in the event of loss or destruction of important files, the corresponding backup copies of the logs are made available within a short period of time.

The CA has implemented a secure backup procedure for the audit logs, performing a weekly backup of all logs using an external device. This external device is stored in a fireproof cabinet under security measures that ensure that only authorized personnel are granted access. Incremental copies are made on a daily basis and full copies on a weekly basis.

Additionally, a copy of the audit logs is in kept in an external custody centre.

5.4.6 Audit information compilation system

Event audit information is compiled internally and automatically by the operating system and the certificate software.

5.4.7 Vulnerability Analysis

The CA carries out regular reviews of any discrepancies in the information contained in the logs and regarding suspicious activities, according to internal procedures established for that purpose in the security policies.

5.5 RECORD ARCHIVE

5.5.1 Type of events archived

Details are retained of the events which take place during the life cycle of the certificate, including its renewal. The CA will store, or delegate the RA to store:

- all audit data
- all data related to certificates, including contracts with subscribers and subscriber identification data
- applications for issuance and revocation of certificates
- all certificates issued or published
- CRLs issued or records of the status of the generated certificates
- documentation required by the auditors
- communications between the components of the PKI

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

5.5.2 Record retention period

All system data relating to the life cycle of certificates must be retained for the period established by relevant legislation where applicable. The issued certificates shall be kept

published in the repository for at least one year following their expiration. Contracts with subscribers and any information on the identification and authentication of the subscriber shall be retained for no less than 15 years or for the period established by applicable legislation.

5.5.3 Archive protection

The CA ensures proper protection of archives by assigning qualified personnel to manage them and through their storage in fireproof safes and in external facilities where required.

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

5.5.4 Archive backup procedures

The CA has an external storage facility to ensure availability of copies of the electronic archive files. The physical documents are stored in secure locations with access restricted to authorized personnel only.

5.5.5 Requirements for time stamping of records

The records are dated with a reliable source.

The CA's technical and configuration documentation contains a section on configuring times on the equipment used in issuing certificates.

5.5.6 Audit information archive system

Not stipulated.

5.5.7 Procedures for obtaining and verifying archived information

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

Access to archived information is provided to authorized personnel only.

The CA will provide the information and media to the auditor for verification of the stored information.

5.6 CA rekeying

5.6.1 Root CA

Prior to the expiry of the Root CA certificate, there will be a change of keys (*rekeying*) and, where appropriate, changes will be made to the content of the certificate which best fit applicable legislation and the reality of Firmaprofesional and the market. The old CA and its private key will only be used for the signature of CRLs while there are active certificates issued by the old CA. A new CA will be generated with a new private key.

The CA's technical and security documentation details the CA's rekeying process.

5.6.2 Subordinate CA

In the case of the subordinate CAs, certificates can be renewed with or without rekeying. The procedures described in the previous paragraph will only apply where rekeying is performed.

5.7 Disaster Recovery Plan

5.7.1 Incident and vulnerability management procedures

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

Any failure to accomplish the goals set by this contingency plan will be treated as being reasonably inevitable unless such failure is due to a breach of the obligations of the CA to implement these processes.

5.7.2 Alteration of hardware resources, software and/or data

In the event that an incident takes place which alters or corrupts hardware resources, software or data, Firmaprofesional will proceed as stipulated in the "Security Policy" document.

5.7.3 Procedure for action in view of vulnerability of a Certification Authority's private key

The contingency plan of Firmaprofesional hierarchy classifies the compromise of the CA's private key as a disaster.

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

- Will notify all subscribers, users and other CAs with which it has agreements or other types of relationship as to the compromise, at a minimum, by means of posting a

notice on the CA's website.

- Will indicate that any certificate or information regarding the status of revocation which has been signed using this key is invalid.

5.7.4 Business continuity after a disaster

The CA will restore critical services (Revocation and publication of revoked certificates) in accordance with this CPS within 24 hours after a disaster or unforeseen emergency, based on the contingency plan and existing business continuity plan.

The CA has an alternative site where, if necessary, the certification systems can be put into operation.

5.8 Cessation of activity

5.8.1 Certification Authority

Before the cessation of its activity the CA will take the following actions:

- It will provide the necessary funds (by means of civil liability insurance) to continue completion of its revocation activities until the definitive cessation of its activity, where applicable.
- It will inform all subscribers, applicants, users, CAs or other entities with which it has agreements or other relationships, with prior notice of no less than 2 months or according to the notice period established by applicable legislation.
- It will revoke all authorizations granted 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, with the express consent of subscribers, transfer the management of the certificates which will remain valid as on the date on which the cessation is due to another certification services provider, which shall assume responsibility for them or otherwise cancel them. The CA will report, where applicable, on the characteristics of the provider to which it is proposes to transfer management of the certificates.
- It shall inform the competent authorities, with the specified advance notice, as to the cessation of its activity and to the destination to be given to the certificates, specifying, where appropriate, whether management is to be transferred and to whom.
- Prior to termination of the activity, it shall provide the competent authorities with

information on the qualified certificates issued to the public whose validity will have been extinguished so that custody can be taken over for the purposes of the provisions of article 20.1.f) of Law 59/2003.

5.8.2 Registration Authority

Prior to the termination of a registration authority of a specific group, Firmaprofesional:

- Shall stop issuing and renewing certificates of that RA.
- Revoke the operator certificates of the RA.
- Revoke the subscriber certificates issued by the RA unless it is expressly decided otherwise.

6 TECHNICAL SECURITY CONTROLS

6.1 Generation and installation of the key pairs

6.1.1 Generation of the key pair

The generation of the key of the **CAs** is performed in accordance with the documented key ceremony process, inside the PSC's secure room, using hardware security modules (HSM). Generation is performed by suitable personnel according to the trusted roles, at least with a dual control and witnesses from Firmaprofesional, from the CA's parent organization and from the external auditor.

For **end entity certificates**, the key generation is performed on devices that provide reasonable assurance that the private key can only be used by the signer, either by physical means or by establishing the subscriber controls and appropriate security measures.

In cases where Firmaprofesional can ensure that the signer's cryptographic keys are created on a Secure Signature Creation Device (SSCD) that meets the requirements of Article 24 of Law 59/2003 on Electronic Signature, is indicated on the certificate itself by including the corresponding OID identifier extension "Certificate Policies".

Otherwise, for example if the private keys have been generated in an Internet browser, the certificates will be issued with OID identifier different.

6.1.2 Delivery of private key to signer

The RA is responsible for ensuring the delivery of the certificate to the signer, either by giving him the signature device or enabling him the download mechanism and subsequent use. The RA must ensure that the signer is in possession of the signature creation data corresponding of the issued certificate.

6.1.3 Delivery of the public key to certificate issuer

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

6.1.4 Delivery of the CA's public key to third parties who rely on the certificates

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

6.1.5 Key size

Certificate	RSA key size (bits)	Validity period (years)
Root CA	4096	21
Subordinate CA	2048	21
End-entity	1024 / 2048	<**>
Operator / Administrator	1024 / 2048	1 (maximum)

A migration of all 1024-bit key length to 2048 bits is in process.

6.1.6 Generation parameters of the public key and quality assurance

The parameters used are those recommended in the technical specifications document issued by ETSI: TS 102 176-1.

Specifically, the parameters used are:

Signature Suite	***Hash Function***	***Padding Method***	***Signature algorithm***
sha1-with-rsa	sha1	emsa-pkcs1-v1.5	rsa
sha256-with-rsa	sha256	emsa-pkcs1-v1.5	rsa

6.1.7 Permitted uses of the key (X.509v3 KeyUsage field)

All certificates include the Key *Usage* and Extended *Key Usage* extension, indicating the approved uses of the keys.

The permitted uses of the key for each certificate are defined in the corresponding Certificate Policy.

6.2 Private key protection and engineering controls of THE CRYPTOGRAPHIC modules

6.2.1 Standards for cryptographic modules

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

The keys of the subscribers of SSCD (DSCF in Spanish) qualified certificates and the keys of operators and administrators are generated securely by the party concerned using a CC EAL4+, FIPS 140-1 level 3, ITSEC E4 High cryptographic device or other equivalent device.

Cryptographic custody devices of the private key of subscribers of SSCD qualified certificates and of the operator or administrator provide a level of security equal to or greater than that

stipulated by applicable legislation for signature data creation devices. The European reference standard for subscriber devices used is CEN CWA 14169.

6.2.2 Multi-person control (k of n) of the private key

Access to the private keys of the CAs simultaneously requires the use of two different cryptographic devices of five possible devices, protected by a password.

6.2.3 Custody of the private key

The private key of the **Root CA** is given custody by a hardware cryptographic device certified with the FIPS 140-2 level 3 standard, ensuring that the private key is never open outside the cryptographic device. The activation and use of the private key requires the multi-person control detailed above. After the operation is performed, the session is closed and the private key remains deactivated.

The private keys of the **Subordinate CA** are kept on secure cryptographic devices certified with the FIPS 140-2 standard level 3.

Firmaprofesional not custody backup copies of the private key certificate subscribers (key escrow).

If the subscriber custody signer's private key, it must be performed using secure cryptographic devices certified to FIPS 140-2 and ensuring at all times the exclusive use of the key by the signer.

6.2.4 Backup copy of the private key

Devices are provided that allow the restoration of the CA's private key; these are stored securely and remain accessible to authorized personnel only according to trusted roles, using at least 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 of 5 cryptographic devices (cards).

This procedure is described in detail in Firmaprofesional security policies.

6.2.5 Private key archive

The CA will not archive the private signature key of certificates after the expiry of its validity period.

The private keys of the internal certificates which use the different components of the CA's system to communicate with each other and to sign and encrypt the data will be archived for a period of at least 10 years after the last certificate is issued.

6.2.6 Transfer of the private key to or from the cryptographic module

A CA key ceremony document is provided which describes the procedures for the generation of the private key and the use of cryptographic hardware.

In other cases, a file can be used in PKCS12 format to transfer the private key to the cryptographic module. In any case, the file is protected by an activation code.

6.2.7 Private key activation method

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

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

6.2.8 Private key deactivation method

Each time you restart the application private keys are automatically disabled

6.2.9 Private key destruction method

Devices which have stored any part of the private key of CA certified signatures, or which have stored the activation data of such keys, are physically destroyed or reinitialized at a low level

6.3 Other aspects of key pair management

6.3.1 Public key archive

The CA will retain all public keys for the period required by applicable legislation, where applicable, or for as long as the certification service is active and for at least 6 months in other cases.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The period of a certificate's use is determined by the period of its validity.

A certificate may not be used after its validity period has elapsed, although the relying party may use it to verify historical data while taking into account that no valid online verification service will be available for that certificate.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Activation data is generated upon the initialization of the cryptographic device.

If initialization takes place in an external entity, the activation data will be delivered to the subscriber through a process which ensures its confidentiality in respect of third parties.

6.4.2 Protection of activation data

Only authorized personnel have knowledge of the activation data of root CA and subordinate CA private keys.

With respect to end-entity certificates, once the device and the activation data have been delivered, it remains the responsibility of the subscriber to maintain the confidentiality of such data.

6.5 IT security controls

The CA deploys reliable systems and commercial products in the provision of its certification services.

The IT equipment used is initially configured with appropriate security profiles by Firmaprofesional system personnel on the following terms:

- Security configuration of the operating system.
- Security configuration of the applications.
- Proper system sizing.
- Configuration of users and permissions.
- Configuration of event logs.
- Backup and recovery plan.
- Antivirus configuration.
- Network traffic requirements.

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

6.5.1 Specific security requirements

Each CA server includes the following features:

- Controlled access to CA services and management of privileges.
- Imposition of segregation of tasks in the management of privileges.
- Identification and authentication of roles associated with identities.
- Archive of subscriber and CA history and audit data.
- Audit of security-related events.
- Security self-diagnosis related to CA services.
- CA system and key recovery mechanisms.

The expounded features are provided through a combination of operating system, PKI software, physical protection and procedures.

6.5.2 Evaluation of IT security

The security of IT equipment is assessed by means of an initial risk analysis, so that the security measures implemented respond to the likelihood and impact produced in the event of security breaches being exploited by a group of identified threats.

Physical security is ensured by the configuration of the facilities described above, whereas the limited number of people working at Firmaprofesional data centre facilitates personnel management.

6.6 Lifecycle security controls

6.6.1 System development controls

The CA possesses a procedure to control changes in the versions of operating systems and applications which imply an enhancement of security features or which correct any detected vulnerabilities.

6.6.2 Security Management Controls

6.6.2.1 Security Management

The CA engages in specific activities to provide training to employees and raise their awareness in matters related to security. The materials used for training and the documents providing descriptions of the processes are updated following their approval by a security

management panel.

The CA requires, under contract, external suppliers involved in certification work to employ equivalent security measures.

6.6.2.2 Classification and management of information and property

The CA maintains an inventory of assets and documentation and a procedure for the management of this material to guarantee its proper use.

The CA's security policy specifies procedures for the management of information which is classified according to its level of confidentiality.

Documents are categorized into three levels: PUBLIC, INTERNAL and CONFIDENTIAL.

6.6.2.3 Management operations

The CA has an appropriate procedure to manage and respond to incidents, through the implementation of an alert system and generation of periodic reports. Incident management procedures are set out in detail in the technical documentation of the CA and of CPD procedures.

The CA has fireproof safes to store physical storage devices.

The CA has an entirely documented procedure regarding the functions and responsibilities of staff involved in the control and manipulation of the elements of the certification process.

6.6.2.4 Handling of storage devices and security

All storage devices will be handled securely in accordance with the requirements of the classification of information. Devices containing sensitive data are securely destroyed where they will not be required again.

6.6.2.5 System planning

The CA'S technical department maintains a record of equipment capabilities.

Together with the application of resource control of each system, it’s possible to make provision for any resizing.

6.6.2.6 Incident and response reports

The CA has a procedure for following up on and resolving incidents where responses are recorded and an economic evaluation is reported which supposes the incident's resolution.

6.6.2.7 Operational procedures and responsibilities

The CA defines the tasks assigned to people with a trusted role separately from personnel responsible for performing daily operations which are not confidential in nature.

6.6.2.8 Access system management

The CA makes every effort reasonably available to them to confirm that access to the system is limited to authorized persons. In particular:

a) Overall management of the CA:

- Controls are available based on high-availability firewalls.
- Sensitive data is protected using cryptographic techniques or access control with strong authentication.
- The CA has a documented procedure for the management of user activations and deactivations and access policy outlined in its security policy.
- The CA has a procedure to ensure that operations are carried out in respect of the roles policy.
- Each person has an associated ID to perform certification operations according to their role.
- The CA's personnel will take responsibility for their actions, for example, by retaining event logs.

b) Certificate generation:

- The CA facilities are equipped with continuous monitoring systems and alarms to detect and record any unauthorized and/or improper attempt to access resources and to enable immediate action.
- The authentication required to perform the issuing process is conducted using an m of n operators system to activate the CA's private key.

c) Revocation management:

- The CA facilities are equipped with continuous monitoring systems and alarms to detect and record any unauthorized and/or improper attempt to access resources of the revocations system and to enable immediate action.
- Revocation means the permanent loss of a digital certificate’s effectiveness.

Revocation is performed subject to card-based strong authentication using the applications of an authorized administrator. Log systems generate the evidence that guarantee non-repudiation of the action taken by the CA operator.

d) Revocation status: the revocation status application is subject to controlled access based on certificate authentication to prevent any attempts to modify revocation status information.

6.6.2.9 Cryptographic hardware life cycle management

- The CA ensures that the cryptographic hardware used to sign certificates is not subject to tampering during transport.
- Cryptographic hardware is built on supports designed to prevent tampering.
- The CA records all relevant information in respect of the device to add to the asset catalogues of Firmaprofesional, S.A.
- The use of cryptographic certificate signing hardware requires the use of at least two trusted employees.
- Firmaprofesional performs periodic tests to ensure that the device is operating properly.
- The cryptographic device is handled by trusted personnel only.
- The CA's private signature key, which is stored in the cryptographic hardware, is deleted once the device is removed.
- The configuration of the CA's system, as well as any modifications and updates thereto, are documented and controlled.
- The CA operates a maintenance contract for the device to provide for its proper maintenance. Changes or updates are authorized by the security manager and are reported in the relevant work records. These settings are affected by at least two trusted personnel.

6.7 Network security controls

The CA protects physical access to network management devices and possesses an architecture that directs the traffic generated on the basis of its security characteristics, by creating clearly defined network sections. This division is achieved through the use of firewalls.

Confidential information which is transferred over non-secure networks is encrypted.

6.8 Time source

The correct time is obtained through consultation with the *Real Observatorio de la Armada* (Spanish Navy Observatory)[18], using NTP protocol over the Internet. The NTP protocol can be found described in RFC 1305 "*Network Time Protocol*".

[18] Information from the website:
http://www.armada.mde.es/ArmadaPortal/page/Portal/ArmadaEspannola/ciencia_observatorio/06_Hora

7 CERTIFICATE, CRL and OCSP PROFILES

7.1 Certificate profiles

The profile of the certificates corresponds to the one put forward in the corresponding certificate policies, and is consistent with the provisions of the following rules:

a) ETSI TS 101 862, known as "European profile for Qualified Certificates"

b) RFC 3280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile",

c) RFC 3739 "Qualified Certificates Profile".

The profile common to call certificates is as follows:

Certificate field	Name	Description
Version	Version No.	*V3 (version of X509 standard)*
Serial	Serial No.	*Random Unique code with respect to the issuer's DN*
Issuer	Issuer	*DN of the CA issuing the certificate*
notBefore	Valid from	*Date on which validly begins, UTC time*
notAfter	Valid until	*Date on which validly ends, UTC time*
Subject	Subject (DN)	*Distinguished name of the subscriber*
Extensions …	Extensions	*Extensions of the certificates.*

7.1.1 Version number

The certificates are in accordance with the X.509 standard, version 3.

7.1.2 Certificate extensions

Extension	Critical	Possible values
X509v3 Basic Constraints	Yes	*2 possible values depending on whether is CA certificate:* CA:FALSE CA:TRUE
X509v3 Key Usage	Yes	Digital Signature Non Repudiation Key Encipherment, Data Encipherment, Key Agreement
X509v3 Extended Key Usage	-	TLS Web Client Authentication E-mail Protection

Extension	Critical	Possible values
X509v3 Subject Key Identifier	-	id of the public key of the certificate obtained from the its hash
X509v3 Authority Key Identifier	-	id of the public key of the certificate of the CA obtained from the its hash
X509v3 CRL Distribution Points	-	URI of the CRL
X509v3 Certificate Policies	-	OID of the certificate policy corresponding to the certificate URI of CPS User Notice : The text which can be displayed on the user's screen
QcStatements	-	There are three types: Id-etsi-qcs-QcCompliance (to be added when certificate is qualifies) Id-etsi-qcs-QcSSCD (indicates that private key is kept in SSCD) id-etsi-qcs-QcLimitValue: Transaction value limit
X509v3 Subject Alternative Name	-	(optional) subscriber's email (o de la CA)
X509v3 Issuer Alternative Name	-	(optional) URI:http://www.firmaprofesional.com
X509v3 Authority Information Access	-	(optional) URI where the CA's certificate is found. (optional) URI of the OCSP service
1.3.6.1.4.1.13177.10.1.5.1.1	-	(Deprecated) Propriety Firmaprofesional extension. You can have the value 'Mancomunado' (Joint) if the signature of the legal person is joint. Where joint signing is not required, the extension will not appear
1.3.6.1.4.1.13177.10.1.5.1.2	-	(Deprecated) Firmaprofesional proprietary extension data which includes subscriber registration data
netscape-cert-type	-	(Deprecated)
netscape-comment	-	(Deprecated)

The extensions presented here correspond to all that may contain the certificates issued. For historical reasons and for compatibility, some extensions containing certificates issued obsolete. In the certification policy of each type of certificate extensions is specified requirements.

7.1.3 Object identifiers (OID) of the algorithms used

OID	Name	Description
1.2.840.113549.1.1.1	rsaEncryption	OID of Public key
1.2.840.113549.1.1.5	sha1withRSAencryption	OID of signature algorithm
1.2.840.113549.1.1.11	sha256withRSAencryption	OID of signature algorithm

7.1.4 Name formats

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

DN field	Name	Description

CN, Common Name	Name	First name and surname(s) of signer, In addition, it may contain a numerical identification code, the signer's tax identification number, distinguishing the value through the inclusion of a prior label "/ num.:" or" - NIF ".
E, E-mail	E-mail	Signer's email
ST, State	Geographic Location	Geographical scope of the signer
C, Country	País	ISO 3166-1 Country code. By default "ES".
serialNumber	Serial Number	Signer's tax identification (NIF) or foreign resident identification (NIE) number*
SN, surName	Surname(s)	Signer's surname(s)
GN, givenName	Given name	Signer Name

If the signer does not have an NIF or NIE, it will contain a document code with the following format <P>-<T>-<XXXXXX>, where:

- <P> is the country code (ISO 3166-1)
- <T> is the document type (passport P)
- <XXXXXXXX> is the code of the document used (the identifier used in the country where the entity to which the subject is linked is registered)

7.1.5 Name restrictions

With respect to certificate encoding, and following the RFC 3280 standard ("Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"), certificates issued on or after 17 April 2008 use *UTF8String* encoding for fields which contain special characters and *PrintableString* for the rest.

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

7.1.6 Certificate Policy Object identifier (OID)

The CPS OID is as follows: 1.3.6.1.4.1.13177.10.0.*X.Y*, where the last 2 digits (X and Y) indicate the version (major and minor respectively) of the document.

The Certificate Policy OIDs of each certificate are listed in the first chapter of the present 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 CPs can be found.
- id-qt-unotice: Note of text which can be displayed on the user's screen during certificate verification.

7.1.8 Semantic processing of "Certificate Policy" extension

The Certificate *Policy* extension enables identification of the policy which Firmaprofesional associates with the certificate and indicates where these policies can be found.

It is composed of 3 elements: the policy OID and the two *PolicyQualifiers* defined above.

7.2 CRL profile

The profile of the CRLs corresponds to the one put forward in the corresponding Certificate Policies, and to standard X.509 version 3 of the RFC 3280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile". The CRLs are signed by the Certification 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 Root authority CRL (Root CA)

FIELDS	VALUES
Version	2
CRL Number	Incremental number
Signature Algorithm	Sha1WithRSAEncryption
Issuer	Distinguished Name (DN) of the issuer
Effective date of issue	(CRL issue date, UTC time)
Date of next update	Effective date of issue+6 months
Authority Key Identifier	Hash of the issuer's key
Only contains user certificates	NO
Only contains issuing entity certificates	NO
Indirect certificate revocation list (CRL)	NO
CRL Entries	Certificate serial number Revocation Date Reason Code

7.2.2.2 CRL of subordinate certificate authorities

FIELDS	VALUES
Version	2
CRL Number	Incremental number
Signature Algorithm	Sha1WithRSAEncryption
Issuer	Distinguished Name (DN) of the issuer
Effective date of issue	(CRL issue date, UTC time)
Date of next update	Effective date of issue+7 days
Authority Key Identifier	Hash of the issuer's key
Only contains user certificates	NO
Only contains issuing entity certificates	NO
Indirect certificate revocation list (CRL)	NO
CRL Entries	Certificate serial number Revocation Date Reason Code

7.3 OCSP profile

The OCSP profile is specified in the secure service (TSA/VA) certificate policy.

8 COMPLIANCE AUDIT AND OTHER CONTROLS

8.1 Frequency of audits

Periodic audits are conducted, generally on an annual basis.

8.2 Auditor qualification

Audits can be either internal or external. In the latter case, these are conducted by companies of recognized prestige in the context of auditing.

Since 2003, Firmaprofesional has been certified with *WEBTRUST for Certification Authorities*, which can be downloaded and consulted at http://www.aicpa.org. This certification is developed by AICPA (American Institute of Certified Public Accountants, Inc.) and CICA (Canadian Institute of Chartered Accountants).

The audit required to obtain WebTrust certification was conducted by the prestigious company Ernst&Young S.L. (Technology and Security Risk Services)

Firmaprofesional is committed to undertaking the necessary audits required to keep this certification current

The WebTrust principles and criteria for CAs are consistent with the standards developed by the American National Standards Institute (ANSI) and the Internet Engineering Task Force (IETF).

Firmaprofesional may establish other auditing criteria, including others commonly accepted in the market for the activity of the CA, or due to establishment of criteria under current regulation.

8.3 Relationship between the auditor and the audited authority

The companies that perform external audits never represent any conflict of interest that may undermine their performance in relation to Firmaprofesional.

However, Firmaprofesional conducts periodic internal audits of the CA of the hierarchy to guarantee its suitability at all times to the requirements set out in the hierarchy's certificate policies.

8.4 Aspects covered by the controls

The audit provides verification of the following principles:

a) **Publication of Information**: That the CA makes public its Business and Certificate Management Practices (the present CPS), as well as its privacy policy with respect to information and personal data protection and that it provides its services in accordance with said statements.

b) **Service Integrity**. That the CA maintains effective controls which provide reasonable assurance:

- That subscriber information is properly authenticated (for the registration activities performed by the CA), and
- Of the integrity of the managed keys and certificates and their protection throughout the life cycle.

c) **General Controls**. That the CA maintains effective controls which provide reasonable assurance that:

- Subscriber and user information is restricted to authorized personnel only and protected from uses not specified in the published business practices of the CA.
- The continuity of operations is maintained with respect to the life cycle management of keys and certificates.

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

8.4.1 Registration authority auditing

Registration Authorities with access to software provided by Firmaprofesional for the management of certificates are audited by a third party prior to its effective implementation. Additionally, audits are conducted to verify compliance with the requirements set forth by the certificate policies for the performance of the registration tasks expounded in the signed service contract. The frequency of audits is determined by agreement between Firmaprofesional and the Registration Authority, always taking into account the activity due to be undertaken by the Registration Authority in terms of the number of certificates or specific security requirements.

Nevertheless, and exceptionally, Firmaprofesional may exempt a Registration Authority from the requirement to undergo an initial audit and maintenance audits.

8.5 Actions to be taken as a result of incident detection

In the event that non-conformities or incidents are detected, appropriate measures shall be deployed to ensure resolution in the shortest time possible. For serious nonconformity

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

In any case, a resolution committee shall be constituted consisting of staff from affected areas and a follow-up committee formed by the heads of the affected areas and General Management.

8.6 Communication of Results

The auditor shall communicate the results to the Technical Director and also to General Director, as the person of ultimate responsibility in Firmaprofesional.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

Prices of certification services or any other service will be communicated to customers or potential customers by Firmaprofesional Sales Department

9.1.2 Certificate access fees

Access to issued certificates is provided free of charge, however, the CA reserves the right to charge a fee in cases of massive downloading of certificates or in any other circumstance which in the opinion of the CA should be made subject to payment.

9.1.3 Fess for access to status or revocation information

Firmaprofesional provides access to information concerning the status of certificates and concerning revoked certificates free of charge, through publication of the corresponding CRL.

Firmaprofesional offers other commercial certificate validation services (such as OCSP or Webservices), whose fees are negotiable with each client of these services.

9.1.4 Fees for other Services

The fees applicable to other services are negotiated between Firmaprofesional and the clients of the services offered.

9.2 Economic Responsibilities

Firmaprofesional, in its activity as a Certification Services Provider, has sufficient financial resources to address the risk of liability for damages and losses caused to the users of their services and to third parties, ensuring the performance of its responsibilities in respect of its PSC activity, as defined in current Spanish legislation.

The above warranty is supported by Liability Insurance with coverage of € 3,000,000.

These guarantees do not apply to unqualified certificates, whereby the amount payable under judicial order in respect of damages and loss is limited to a maximum of € 6,000.

9.3 Confidentiality of information

Firmaprofesional has an appropriate policy for the handling of information and appropriate agreement models which all personnel having access to confidential information are bound to sign.

Firmaprofesional complies, in all cases, with current legislation in respect of data protection and specifically the provisions of Law 15/1999 of 13 December on the Protection of Personal Data.

In accordance with the provisions of Article 19.3 of Law 59/2003 on Electronic Signatures, this CPS shall be considered the "Documento de Seguridad" (Security Document) for the purposes specified in data protection legislation and associated regulation.

9.3.1 Scope of confidential information

Firmaprofesional considers all information which is not explicitly indicated as public information as being confidential information. No disclosure shall be made in respect of information declared as confidential without the express written consent of the entity or organization that has assigned it with the character of confidentiality, except where there is a legal requirement to do so.

9.3.2 Non-confidential information

The following information will be considered non-confidential:

- Information contained in the present CPS.
- Information contained in different Certificate Policies (CP).
- The information contained in the certificates, given that subscribers give their prior consent for their issue, including the certificate's various statuses or conditions.
- The certificate revocation lists (CRL's), as well as other revocation status information.
- The information contained in the certificate deposits.
- Any information whose publication is imposed by regulation.

9.3.3 Responsibility to protect confidential information

It remains the responsibility of Firmaprofesional to establish appropriate measures for the protection of confidential information.

9.4 Protection of personal information

9.4.1 Personal data protection policy

In compliance with the requirements of Law 15/1999 of 13 December on the protection of personal data, Firmaprofesional has the BB DD CERTIFICADOS file, whose purpose is the management of certificates issued and the provision of associated certification services.

File information:

Name	BB DD CERTIFICADOS
Registration Number in the *Registro General de Protección de Datos* (General Data Protection Register)	2022130054
Customer service	Edificio ESADECREAPOLIS - 1B13. Avenida Torre Blanca, 57. Sant Cugat del Valles 08173

9.4.1.1 Aspects covered

This document describes the procedures, requirements and obligations regarding the compilation and management of personal data in compliance with the provisions of Law 15/1999 of 13 December on the Protection of Personal Data, and Royal Decree 1720/2007 of 21 December, which approves the regulation implementing Organic Law 15/1999, of 13 December, on the protection of personal data.

Specifically, the following sections covered by ***TITLE VIII "Regarding security measures in the processing of personal data" of Royal Decree 1720/2007*** are fulfilled in the specified sections of the present document and in the Security Policy document:

- Scope of the security document → section 9.4
- Application of the levels of security → sections 5, 6 and 9.4
- The functions and obligations of staff → section 5.3
- Structure of the filing systems with personal data → section 9.4
- Procedure of notification, management and response to incidents → Security Policy
- Backup copies and recovery of data → Security Policy

Compliance is thereby ensured with the provisions of Article 19.3 of Law 59/2003 of 19 December on electronic signatures, which considers the certification practice statement as a security document for the purposes provided for in personal data protection legislation.

9.4.2 Information treated as private

In accordance with the provisions of Article 3 of Law 15/1999 of 13 December on the protection of personal data, Personal data means any information concerning identified or identifiable natural persons.

Personal information not included in the certificates and in the mechanism described for checking certificate status, is considered personal data of a private nature.

The following data is, in all circumstances, considered as private information:

- Approved or denied certificate applications, and any other personal information obtained for the purposes of issuance and maintenance of certificates, except the information specified in the corresponding section.
- Private keys generated and/or stored by the Certification Authority.
- Any other information identified as private.

In any case, the data obtained by the Certification Services Provider shall be handled according to the basic security level.

9.4.2.1 Structure of personal files

Personal scope	Given name and surname(s)
	E-mail
	Place and Date of Birth
	Country
	National ID Number (DNI)
Professional scope	Tax Identification Number (CIF) corresponding to the person or entity to which the subscriber is connected
	Department or unit to which the signer belongs
	Position, title or role of the signer in the organization
	Geographic location of signer in the organization (company or association)
	Employee or professional membership number

9.4.3 Information not classified as private

The following information is not classified as private:

- The information contained in the certificates, given that subscribers give their prior consent for their issue, including the certificate's various statuses or conditions.

- The certificate revocation lists (CRLs), as well as other revocation status information.

9.4.4 Responsibility for the protection of personal data

Confidential information under the LOPD (Data Protection Law) is protected from loss, destruction, damage, falsification and unauthorized or unlawful processing, in accordance with the requirements established by Royal Decree 994/99, of 11 June, which approves the Regulation on Mandatory Security Measures for the Computer Files which contain Personal Data.

9.4.5 Communication and consent to use personal data

The user's authorization for the processing of personal data supplied for the provision of agreed services and for the supply and acquisition of other products and services of Firmaprofesional, S.A, is required through the signing and acceptance of the legally binding instrument.

The information obtained is used for the correct identification of users requesting personalized services, for conducting statistical studies of registered users with a view to designing improvements in the services provided, to perform basic administrative tasks and to report incidents, news and special offers to registered users via email.

The personal information of registered users is stored in the data base that is the property of Firmaprofesional, with deployment of the technical, organizational and security measures required to ensure the confidentiality and integrity of information in accordance with the provisions of Law 15/1999 of 13 December on the Protection of Personal Data, and other applicable legislation.

The user is responsible, in all cases, for the veracity of the data provided, whereas Firmaprofesional reserves the right to deny services to any user who has provided false information, notwithstanding any other legal action.

Any registered user may, at any time, exercise their right to access, correct and, where necessary, remove their personal data, as provided to Firmaprofesional, by means of a written request with the reference "tratamiento de datos" (data processing).

9.4.6 Disclosure in the context of a judicial process

Personal data may be disclosed by Firmaprofesional without the prior consent of the subscriber in the context of a judicial procedure in respect of the cases referred to in paragraph 2 of Article 11 of Law 15/1999 of 13 December on the Protection of Personal Data.

9.4.7 Other circumstances of information disclosure

Those described in paragraph 2 of Article 11 of Law 15/1999 of 13 December on the Protection of Personal Data.

9.5 Intellectual property rights

a) Property of the CPS

The intellectual property of this CPS and the different CPs belong to Firmaprofesional, S.A.

b) Property of the certificates

Firmaprofesional will be the only entity to enjoy intellectual property rights over the certificates which it issues unless explicitly stated otherwise.

Firmaprofesional grants non-exclusive permission to reproduce and distribute certificates, free of charge, provided that the reproduction is integral and does not alter any element of the certificate, and where such is necessary in connection with digital signatures and/or encryption systems within the context of this policy and in accordance with the relevant binding instrument made between Firmaprofesional and the party which reproduces and/or distributes the certificate, as well as with the corresponding general conditions of issue.

c) Ownership of keys

The pair of keys is the property of the subscriber.

The above rules are set out in the binding instruments made between the CAs and the subscribers and third parties who rely on certificates.

9.6 Obligations

9.6.1 Obligations of the CA

Firmaprofesional is bound, in accordance with this document and with the provisions of regulation governing the provision of Certification services and Law 59/2003, in particular, to:

a) Respect the provisions of the Policies and Practices of Certification (this CPS) and the General Conditions of issue.

b) Publish this CPS on its website.

c) Give notice of amendments to the CPS to subscribers to the RAs that are thereby

bound and to users, through the publication of said amendments on its website.

d) Maintain civil liability insurance with the minimum coverage required by current regulation.

e) Use reliable systems to store qualified certificates, enabling verification of their authenticity and preventing unauthorized alteration of the data, restricting access under the terms and to the persons indicated by the signer and enabling the detection of any changes to these security conditions.

As regards to certificates:

d) Issue certificates under this CPS and applicable standards.

e) Issue certificates based on information in its possession and free from data-entry errors.

f) Issue certificates with the minimum content established by applicable regulation, where applicable.

g) Publish the certificates issued in a Record of Certificates, always respecting the provisions related to data protection under current regulation.

h) Suspend and revoke certificates in accordance with the CPS and publish such revocations in the CRL (Certificate Revocation List).

Regarding custody of information:

i) Retain information on issued certificates for the minimum period required by current regulations, where applicable.

j) Do not store or copy subscribers' signature creation data, where so stipulated in current regulations.

k) Protect, with due care, signature creation data while in its custody, where applicable.

l) Protect the private keys in a secure manner.

m) Establish mechanisms for generation and custody of the relevant information on the activities described, protecting them against loss, destruction or falsification.

9.6.2 Obligations of the RA

The registration authorities are also obliged under the terms defined in this CPS for the issuance of certificates, in particular, to:

a) Respect the provisions of this CPS and the CP corresponding to the type of certificate issued.

b) Comply with the provisions set forth in the contracts signed with the CA.

c) Comply with the provisions set forth in the contracts signed with the Subscriber.

During the life cycle of the certificates:

d) Verify the identity of certificate applicants as described in this CPS or in accordance with another process which has been approved by Firmaprofesional.

e) Verify the accuracy and authenticity of the information provided by the subscriber or applicant.

f) Inform the applicant, before issuing a certificate, of the obligations thereby assumed, the way in which the signature creation data must be safeguarded, the procedure to be followed in reporting the loss or misuse of data or signature creation and verification devices, its price, the necessary conditions for the use of the certificate, its limitations of use and how to guarantee their potential pecuniary liability, and the web page where all information with respect to Firmaprofesional, the CPS and the CP corresponding to the certificate can be consulted.

g) Process and deliver certificates as stipulated in this CPS and in the corresponding CP.

h) Formalize the certificate contract with the subscriber as established by the applicable Certificate Policy.

i) Pay the fees established for the requested certification services.

j) Maintain the documents provided by the subscriber archived for the period stipulated in current legislation.

k) Inform the CA of the causes of revocation, whenever and provided that they have such knowledge.

l) Communicate with subscribers, by means considered appropriate, with a view to the proper life-cycle management of the certificates. Specifically, to provide notifications relating to the proximity of the expiration of certificates and the suspension, restitution and revocation thereof.

9.6.3 Obligations of applicants

An applicant for a certificate shall be bound to comply with the provisions of legislation and also to:

a) Provide the RA with the information necessary to conclude correct identification.

b) Make every effort that is reasonably within their power to confirm the accuracy and veracity of the information provided.

c) Report any changes in the data provided for the creation of the certificate during its period of validity.

d) Comply with the provisions in the contract documents signed with the CA and the RA.

9.6.4 Obligations of signers

The signer is bound to comply with current regulations and also to:

a) Keep custody of their SSCD, private keys and secure codes in a diligent manner.

b) Use the certificate as provided for in the present CPS.

c) Respect the provisions of legally binding instruments with the CA and RA.

d) Report, as quickly as possible, the existence of any grounds for suspension or revocation.

e) Report any changes occurring to the data provided for the creation of the certificate during its period of validity.

f) Refrain from using the private key and the certificate as soon as a request is made for the suspension or revocation thereof or following notice of such suspension or revocation by the CA or RA, or upon expiry of the period of the certificate's validity.

9.6.5 Obligations of third parties who rely on certificates

Users are bound to comply with current regulations and, further, to:

a) Verify the validity of certificates when performing any operation based thereon.

b) Be informed of and comply with the guarantees, limits and responsibilities applicable in respect of the acceptance and use of certificates on which it relies, and agree to comply therewith.

9.7 Disclaimer of Warranty

Firmaprofesional may disclaim any guarantee of service which is not linked to the obligations established by Law 59/2003 of 19 December.

9.8 Liabilities

9.8.1 Liabilities of the Certification Authority

Firmaprofesional, in respect of its business of providing certification services, may be held liable for any breach of the provisions established in the Policies and Practices of certification and where applicable, for the provision set forth in Law 59/2003 of 19 December on electronic signatures or its implementing regulations.

Notwithstanding the above, Firmaprofesional does not guarantee the cryptographic algorithms and standards used and shall not be held liable for any damage caused by external attacks thereon, provided that due diligence has been implemented according to the state of the art at all times and provided that it has acted in accordance with the provisions of this CPS and Law 59/2003 of 19 December on electronic signature and its implementing regulations, where applicable.

Firmaprofesional may be held liable for damage caused with respect to the Subscriber or any person who relies in good faith on the certificate, provided that there is intent or gross negligence, in respect of:

- The accuracy of the information contained in the certificate on the date of issue, where this corresponds to authenticated information.
- The guarantee that the public and private key function in conjunction and in a complementary manner.
- The correspondence between the requested certificate and the delivered certificate.
- Any liability which is established by applicable legislation.

9.8.2 Responsibilities of the Registration Authority

The RA will assume all responsibility in the subscriber identification process and the verification of their identity. For such purpose, it shall act in accordance with the provisions of the present CPS or in accordance with another procedure which has been approved by Firmaprofesional.

In the event that the generation of the key pairs is not performed in the presence of the subscriber, the RA shall be responsible for the custody of the keys until their delivery to the subscriber.

9.8.3 Subscriber Responsibilities

It is the responsibility of the Subscriber to comply with the obligations set forth in this

document, in the corresponding CP, and in the legally binding instrument.

9.8.4 Limitation of liabilities

Firmaprofesional shall not be held liable in any respect in the event of any of these circumstances:

a) State of war, natural disasters, defective functioning of electricity services, data communications and/or telephone networks or computer equipment used by the Subscriber or by third parties, or any other case of force majeure.

b) Misuse or fraudulent use of the certificates directory and the CRLs (Certificate Revocation List) issued by the Certification Authority.

c) The misuse of information contained in the Certificate or CRL.

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

e) In relation to any acts or omission practiced by the Applicant and Subscriber:

- Lack of accuracy or veracity of the information provided to issue the certificate
- Delay in notification of the grounds for suspension or revocation of the certificate
- Absence of request for suspension or revocation of the certificate where applicable
- Negligence in the maintenance of signature creation data, in ensuring its confidentiality and in its protection against access or disclosure.
- Use of the certificate outside the period of its validity, or when Firmaprofesional or the RA gives notice of its revocation or suspension.
- Breach of the limitations of use of the certificate, according to current regulations and the present CPS, in particular, exceeding the limits described in the electronic certificate with regard to its possible uses and the amount of an individual transaction which may be performed with the certificate or any use which does not comply with the conditions established and communicated to the signer by Firmaprofesional.

f) In relation to acts or omissions of a third party who relies on the certificate:

- Failure to verify the restrictions contained in the electronic certificate or in the present CPS in terms of its potential uses and the amount of an individual

transaction which it can be used to perform.

- Failure to verify the suspension or loss of validity of the electronic certificate published in the consultation service regarding the validity of the certificates or failure to verify the electronic signature.

9.9 Compensation

9.9.1 Scope of Coverage

The insurance will pay all amounts which Firmaprofesional S.A. is rendered legally obligated to pay, up to the contracted limit of its coverage, as a consequence of any legal procedure in which it may be declared liable, resulting from any negligent act, error or unintentional failure to comply with applicable legislation among others.

9.9.2 Insurance coverage or guarantees for relying parties

No coverage exists with respect to relying parties.

9.9.3 Loss Limitations

Firmaprofesional limits its liability by establishing restrictions on the use of the certificate and limits on the value of the transactions in which the certificate may be used, as expressed in the certificates themselves by means of the *qcStatements* extension (OID 1.3.6.1.5.5.7.1.3) and in the corresponding CP.

Where the subscriber sees fit, he/she may request and if necessary agree a limit which is higher than the one indicated, incurring additional costs where this is established. In addition, the subscriber or third parties may enter into bilateral agreement or agree on specific coverages for transactions of a higher value, whereas, in such cases, the limit of liability of the CA indicated in the preceding paragraphs shall remain unaltered, in accordance with the applicable certificate policy.

9.10 Period of validity

9.10.1 Period

The CPS and the different CPs enter into force upon their publication.

9.10.2 Replacement and repeal of the CPS

The present CPS and the various CPs will be repealed at such time as a new version of the document is published.

The new version shall fully replace the previous document.

9.10.3 Effects of termination

With regard to current certificates issued under a previous CPS or CP, the new version will prevail over the previous version.

9.11 Individual notices and communications with participants

In the legally binding instrument with the subscriber, Firmaprofesional establishes the means and time limits for notifications.

In general, use is made of Firmaprofesional website www.firmaprofesional.com to perform any type of notification or communication.

9.12 Changes in the specifications

9.12.1 Procedure for the changes

9.12.1.1 Elements that can change without notice

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

9.12.1.2 Changes with notification

Any element of this CPS may be changed unilaterally by Firmaprofesional without prior notice. The amendments should be reasoned from a legal, technical or commercial standpoint.

9.12.1.3 Notification Mechanism

All proposed changes which may substantially affect subscribers, users or third parties shall be notified immediately to interest parties though publication on Firmaprofesional website.

The RA will be notified directly by email or telephone depending on the nature of the implemented changes.

9.12.2 Notification period and procedure

The people, institutions or entities affected may submit comments to the organization of the administration of policies within a period of 45 days following notification.

It remains at the discretion of the organization responsible for the administration of policies whether and what action should be taken as a result of any comments.

9.12.3 Circumstances under which the OID must be changed

The OID shall be altered in any circumstances where there is alteration to any procedure which is described in the present document or in any of the CPs and which directly affects the operating mode of any of the participating entities.

9.13 Complaints and dispute resolution

For the resolution of any dispute arising in connection with this document, the CPs or the legally binding document, the parties waive any other jurisdiction to which they may be entitled, and submit themselves to the Corte Española de Arbitraje (Spanish Arbitration Court).

9.14 Applicable legislation

The legislation applicable to the present document, as well as to the various CPs, and to the operations that derive therefrom, is 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 (eIDAS) and repealing Directive 1999/93/EC
- Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.
- Law 59/2003 of 19 December on electronic signatures.
- Law 11/2007 of 22 June, on Citizens' Electronic Access to Public Services
- Organic Law 15/1999 of 13 December on the protection of personal data.
- Royal Decree 1720/2007 of 21 December which approves the regulation implementing Organic Law 15/1999 of 13 December on the protection of personal data.

9.15 Compliance with applicable regulations

Firmaprofesional manifests its compliance with law 59/2003 of 19 December on electronic signatures.

9.16 Miscellaneous Provisions

9.16.1 Full acceptance clause

All third parties who rely on the certificates thereby accept the content of the latest version of this document and the corresponding CP in its entirety.

9.16.2 Severability

The invalidity of one of the clauses in this CPS will not affect the remainder of the document. In this case, the mentioned clause shall be null and void.

9.16.3 Court Resolution

Any dispute or conflict which may arise from the present document shall be resolved through arbitration within the framework of the *Corte Española de Arbitraje* (Spanish Arbitration Court) in conformity with its Regulations and Statutes, governing the administration and conduct of the arbitration and the nomination of the arbitrator or the arbitrator tribunal. The parties state their undertaking to comply with the decision rendered.