PKI Disclosure Statement (PDS)

Firmaprofesional disclosure statement of Personal, Corporate, Public Administration, Body or Public Law Entity certificates

Version: 230216

Classification: Public

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

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

WWW.FIRMAPROFESIONAL.COM

Use and disclosure restrictions regarding the data contained in this document

This document contains essential information regarding the certification service of FIRMAPROFESIONAL Certification Entity.

Version history

Version	Section and changes	Date
170220	• Creation of the document.	20/02/2017
190220	• Annual revision. • Adaptation to the new template. • Incorporation of the Policies referral for each certificate.	20/02/2019

190612	• Added sections:
	  ○ "*2.15. Corporate Certificate with Company Seal for PSD2*"
	  ○ "*2.17. SSL EV for PSD2*"
	• Renumbering the affected sections.
	• (*Exclusively in English version*) Unified terminology for "Professional Association".
		12/06/2019

200123	The wording of the following sections is improved, for clarity and documental consistency: • "2.29 Medium-Level Body Seal Certificate issued within Other Devices" • "3.2 Usage Limitations for Verifiers" • "4.1 Key Generation"	23/01/2020
210217	Adaptation to the new Law 6/2020, regulating certain aspects of electronic trust services.	17/02/21
220217	Annual Review	17/02/22
230216	Annual Review	16/02/23

Index

1. Contact information

1.1. Responsible Organization

The Certification Entity FIRMAPROFESIONAL, henceforth "FIRMAPROFESIONAL" is an initiative of:

FIRMAPROFESIONAL, S.A.

Calle Paseo Bonanova 47,

08017 Barcelona.

Tel: (+34) 902 361 639

1.2. Contact

For any query, contact:

FIRMAPROFESIONAL, S.A.

Calle Paseo Bonanova 47,

08017 Barcelona.

Tel: (+34) 902 361 639

1.3. Contact for renewal processes

For any query, contact :

FIRMAPROFESIONAL, SA.

Tel: (+34) 902 361 639

2. Certificate types and purposes

2.1. Personal Certificate

Qualified certificates for physical person/s that identify a subscriber and a signatory as the same physical person needing to conduct processes towards Public Administrations and other institutions.

Regarded as qualified certificates due to the fact that they comply with requirements established in Annex I of Regulation (EU) 910/2014.

Identified with the OID number: 1.3.6.1.4.1.13177.10.1.40.2

Included in the Certification Policy on Electronic Signature Certificates.

These certificates shall not include a QcStatement extension with the value set as "id-etsi-qcs-QcSSCD".

2.2. Corporate Certificate for a Professional Association Member issued within a Portable QSCD

Qualified certificates for physical person/s that identify a subscriber as the Professional Association, and the signatory as the member of the corresponding Professional Association.

Regarded as qualified certificates due to the fact that they comply with requirements established in Annex I of Regulation (EU) 910/2014.

Identified with the OID number: 1.3.6.1.4.1.13177.10.1.1.1

Included in the Certification Policy for Electronic Signature Certificates.

The cryptographic keys of the signatory are created within a portable Qualified Signature Creation Device (QSCD), in compliance with requirements established in Annex II of EU Regulation 910/2014, and with the QcStatement extension set with the value, "id-etsi-qcs-QcSSCD".

2.3. Corporate Certificate for a Professional Association Member issued within a Centralized QSCD

Qualified certificates for physical person/s that identify a subscriber as the Professional Association, and the signatory as the member of the corresponding Professional Association.

Regarded as qualified certificates due to the fact that they comply with requirements established in Annex I of Regulation (EU) 910/2014.

Identified with the OID number: 1.3.6.1.4.1.13177.10.1.1.3

Included in the Certification Policy for Electronic Signature Certificates.

The cryptographic keys of the signatory are created within a centralized Qualified Signature Creation Device (QSCD) in compliance with requirements established in Annex II of EU Regulation 910/2014, and with the QcStatement extension set with the value, "id-etsi-qcs-QcSSCD".

2.4. Corporate Certificate of a Professional Association Member issued within Other Devices

Qualified certificates for physical person/s that identify a subscriber as the Professional Association, and the signatory as the member of the corresponding Professional Association.

Regarded as qualified certificates due to the fact that they comply with requirements established in Annex I of Regulation (EU) 910/2014.

Identified with the OID number: 1.3.6.1.4.1.13177.10.1.1.2

These certificates shall not include a QcStatement extension with the value set as "id-etsi-qcs-QcSSCD".

2.5. Corporate Certificate for Physical Person/s issued within a Portable QSCD

Qualified certificates for physical person/s that identify a subscriber as a Corporation and the signatory as a physical person associated with the Corporation, whether an employee, associate, collaborator, client, supplier or a person having another type of relationship.

Qualified certificates due to the fact that they comply with requirements established in Annex I of Regulation (EU) 910/2014

Identified with the OID number: 1.3.6.1.4.1.13177.10.1.2.1

Included in the Certification Policy on Electronic Signature Certificates.

The cryptographic keys of the signatory are created within a portable Qualified Signature Creation Device (QSCD) in compliance with requirements established in Annex II of EU Regulation 910/2014, and with the QcStatement extension set with the value, "id-etsi-qcs-QcSSCD".

2.6. Corporate Certificate of a Physical Person Issued on a Centralized QSCD

Qualified certificates for physical person/s that identify a subscriber as a Corporation and the signatory as a physical person associated with the Corporation, whether an employee, associate, collaborator, client, supplier or a person having another type of relationship.

Qualified certificates due to the fact that they comply with requirements established in Annex I of the Regulation (UE) 910/2014.

Identified with OID number: 1.3.6.1.4.1.13177.10.1.2.3

Included in the Certification Policy on Electronic Signature Certificates.

The cryptographic keys of the signatory are created within a centralized Qualified Signature Creation Device (QSCD) in compliance with requirements established in Annex II of EU Regulation 910/2014, and with the QcStatement extension set with the value, "id-etsi-qcs-QcSSCD"

2.7. Corporate Certificate of a Physical Person Issued within Other Devices

Qualified certificates for physical person/s that identify the subscriber as a Corporation and the signatory as a physical person associated with the Corporation, whether an employee, associate, collaborator, client, supplier or a person having another type of relationship.

Qualified certificates due to the fact that they comply with the requisites established in Annex I of Regulation (EU) 910/2014)

Identified with the OID number: 1.3.6.1.4.1.13177.10.1.2.2 and 1.3.6.1.4.1.13177.10.1.14.2 (with use to sign emails).

Included in the Certification Policy on Electronic Signature Certificates.

These certificates shall not include a QcStatement extension with the value set as "id-etsi-qcs-QcSSCD"

2.8. Corporate Certificate for Legal Representative issued within Portable QSCD

Qualified certificates for physical person/s that identify the subscriber as a Corporation and the signatory as a legal representative of the Corporation

Qualified certificates due to the fact that they comply with requirements established in Annex I of Regulation (UE) 910/2014.

Identified with the OID number: 1.3.6.1.4.1.13177.10.1.11.1

Included in the Certification Policy on Electronic Signature Certificates.

The cryptographic keys of the signatory are created within a portable Qualified Signature Creation Device (QSCD) in compliance with requirements established in Annex II of EU Regulation 910/2014, and with the QcStatement extension with the value, "id-etsi-qcs-QcSSCD".

2.9. Corporate Certificate for Legal Representative issued within a Centralized QSCD

Qualified certificates for physical person/s that identify the subscriber as a Corporation and the signatory as a legal representative of the Corporation

Qualified certificates due to the fact that they comply with requirements established in Annex I of Regulation (EU) 910/2014.

Identified with the OID number: 1.3.6.1.4.1.13177.10.1.11.3

Included in the Certification Policy for Electronic Signature Certificates.

The cryptographic keys of the signatory are created within a centralized Qualified Signature Creation Device (QSCD) in compliance with requirements established in Annex II of EU Regulation 910/2014, and with the QcStatement extension with the value, "id-etsi-qcs-QcSSCD".

2.10. Corporate Certificate of Legal Representative issued within Other Devices

Qualified certificates for physical person/s that identify the subscriber as a Corporation and the signatory as a legal representative of the Corporation

Qualified certificates due to the fact that they comply with requirements established in Annex I of Regulation (EC) 910/2014.

Identified with OID number: 1.3.6.1.4.1.13177.10.1.11.2

Included in the Certification Policy for Electronic Signature Certificates.

These certificates shall not include a QcStatement extension with the value set as "id-etsi-qcs-QcSSCD"

2.11. Corporate Certificate for Voluntary Representative issued within Portable QSCD

Qualified certificates for physical person/s that identify the subscriber as a Corporation and the signatory as a voluntary representative of the Corporation empowered towards public administrations.

Qualified certificates due to the fact that they comply requirements established in Annex I of the Regulation (EU) 910/2014.

Identified with the OID number: 1.3.6.1.4.1.13177.10.1.12.1

Included in the Certification Policy on Electronic Signature Certificates.

The cryptographic keys of the signatory are created within a portable Qualified Signature Creation Device (QSCD) in compliance with requirements established in Annex II of EU Regulation 910/2014, and with the QcStatement extension with the value, "id-etsi-qcs-QcSSCD".

2.12. Corporate Certificate of a Voluntary Representative on a Centralized QSCD

Qualified certificates for physical person/s that identify the subscriber as a Corporation and the signatory as a voluntary representative of the Corporation empowered towards public administrations.

Qualified certificates due to the fact that they comply requirements established in Annex I of the Regulation (EU) 910/2014.

Identified with OID number: 1.3.6.1.4.1.13177.10.1.12.3

Included in the Certification Policy on Electronic Signature Certificates.

The cryptographic keys of the signatory are created within a centralized Qualified Signature Creation Device (QSCD) in compliance with requirements established in Annex II of EU Regulation 910/2014, and with the QcStatement extension set with the value, "id-etsi-qcs-QcSSCD".

2.13. Corporate Certificate for Voluntary Representative issued within Other Devices

Qualified certificates for physical person/s that identify the subscriber as a Corporation and the signatory as a voluntary representative of the Corporation empowered towards public administrations.

Qualified certificates due to the fact that they comply requirements established in Annex I of the Regulation (EU) 910/2014.

Identified with the OID number: 1.3.6.1.4.1.13177.10.1.12.2

Included in the Certification Policy on Electronic Signature Certificates.

These certificates shall not include a QcStatement extension with the value set as "id-etsi-qcs-QcSSCD".

2.14. Corporate Certificate with Company Seal

Electronic certificates issued to legal persons in accordance with Article 39 of EU Regulation 910/2014.

The purpose of these certificates is to be able to automatically sign electronic documents on behalf of a legal person.

Qualified certificates due to the fact that they comply with the requisites established in Annex I of the Regulation (EU) 910/2014.

Identified with the OID number: 1.3.6.1.4.1.13177.10.1.10.2

Included in the Certification Policy for Electronic Seal Certificates.

These certificates shall not include a QcStatement extension with the value set as "id-etsi-qcs-QcSSCD"

2.15. Corporate Certificate with Company Seal for PSD2

Electronic certificates issued to payment services provider.

The purpose of these certificates is to be able to automatically sign electronic documents on behalf of the payment service provider, which can be:

- Account Servicing Payment Service Provider (PSP_AS)
- Payment Initiation Service Provider (PSP_PI)
- Account Information Service Provider (PSP_AI)
- Issuer of card-based payment instruments

Qualified certificates due to the fact that they comply with the requisites established in Annex I of the Regulation (EU) 910/2014.

Identified with the OID number: 1.3.6.1.4.1.13177.10.1.10.2

Included in the Certification Policy for Electronic Seal Certificates.

These certificates shall not include a QcStatement extension with the value set as "id-etsi-qcs-QcSSCD"

2.16. SSL EV Certificate

These certificates are issued for Web servers created according to specific criteria for verifying the identity of the organization defined in the certificate.

EV-SSL Certificates allow browsers connecting to this service to display an additional level of security to that provide by standard SSL certificates.

Qualified certificates due to the fact that they comply with requirements established in Annex I of EU Regulation 910/2014.

Identified with OID number: 1.3.6.1.4.1.13177.10.1.3.10

Included in the Certification Policy for Website Authentication Certificates.

2.17. SSL EV Certificate for PSD2

These certificates are issued to servers at the request of payment service providers that are registered by the Competent National Authority,and are issued in accordance with a specific set of criteria to verify the identity of the organization identified in the certificate.

Qualified certificates due to the fact that they comply with requirements established in Annex I of EU Regulation 910/2014.

Identified with OID number: 1.3.6.1.4.1.13177.10.1.3.10

Included in the Certification Policy for Website Authentication Certificates.

2.18. TSA/VA Certificate

Qualified certificates that permit signing digital evidence such as the Time Stamping Authority (TSA) or the Validation Authority (VA), according to requirements established within Articles 41 and 42 of EU Regulation EU 910/2014.

Identified with the OID number: 1.3.6.1.4.1.13177.20.0.1

These are qualified certificates due to the fact that they comply with requirements established in Annex I of Regulation (EU) 910/2014.

Included in the Certification Policy for Secure Service Certificates.

The cryptographic keys of the signatory are created within a centralized Qualified Signature Creation Device (QSCD) in compliance with requirements established in Annex II of EU Regulation 910/2014, and with the QcStatement extension set with the value, "id-etsi-qcs-QcSSCD".

2.19. High-level Certificate for Public Servant issued within Portable QSCD

Qualified certificates issued to public servant that identify the subscriber as a Public Administration, and the signatory as the physical person within the service of that public administration.

Comply with requirement established in Article 43 of Act 40/2015 of October 1st Public Sector Legal Regime for electronic signatures of personnel within the service of Public Administrations.

Qualified certificates due to the fact that they comply with requirements established in Annex 1 of the Regulation (EU) 910/2014.

Identified with the OID number: 1.3.6.1.4.1.13177.10.1.22.1

According to the spanish regulation, these certificates are identified with OID number: 2.16.724.1.3.5.7.1

Included in the Certification Policy for Electronic Signature Certificates.

The cryptographic keys of the signatory are created within a portable Qualified Signature Creation Device (QSCD) in compliance with requirements established in Annex II of EU Regulation 910/2014, and with the QcStatement extension set with the value "id-etsi-qcs-QcSSCD".

2.20. High-level Certificate for Public Servant issued within Centralized QSCD

Qualified certificates issued to public servant that identify the subscriber as a Public Administration, and the signatory as the physical person within the service of that public administration.

Comply with requirement established in Article 43 of Act 40/2015 of October 1st Public Sector Legal Regime for electronic signatures of personnel within the service of Public Administrations.

Qualified certificates due to the fact that they fulfill the requisites established in Annex I of the Regulation (EC) 910/2014.

Identified with OID number: 1.3.6.1.4.1.13177.10.1.22.3

According to the spanish regulation, these certificates are identified with OID number: 2.16.724.1.3.5.7.1

Included in the Certification Policy on Electronic Signature Certificates.

The cryptographic keys of the signatory are created within a centralized Qualified Signature Creation Device (QSCD) in compliance with requirements established in Annex II of EU Regulation 910/2014, and with the QcStatement extension set with the value "id-etsi-qcs-QcSSCD".

2.21. Medium-Level Certificate for Public Servant

Qualified certificates issued to public servant that identify the subscriber as a Public Administration, and the signatory as the physical person within the service of that public administration..

Comply with requirement established in Article 43 of Act 40/2015 of October 1st Public Sector Legal Regime for electronic signatures of personnel within the service of Public Administrations.

Identified with OID number: 1.3.6.1.4.1.13177.10.1.22.2

According to the spanish regulation, these certificates are identified with OID number: 2.16.724.1.3.5.7.2

Included in the Certification Policy for Electronic Signature Certificates.

These certificates shall not include a QcStatement extension with the value set as "id-etsi-qcs-QcSSCD"

2.22. High-level Certificate for Public Servant with Pseudonym issued within Portable QSCD

Qualified certificates issued to public servant with pseudonym that identify the subscriber as a Public Administration, and the signatory as the physical person within the service of that public administration..

The physical person is identified by their professional identification number. Identification of the public servant via first name, last name or Tax Identification Number is prohibited.

Comply with requirement established in Article 43 of Act 40/2015 of October 1st Public Sector Legal Regime for electronic signatures of personnel within the service of Public Administrations.

Qualified certificates due to the fact that they comply with requirements established in Annex I of Regulation (EU) 910/2014.

Identified with the OID number: 1.3.6.1.4.1.13177.10.1.23.1

According to the spanish regulation, these certificates are identified with OID number: 2.16.724.1.3.5.4.1

Included in the Certification Policy for Electronic Signature Certificates.

The cryptographic keys of the signatory are created within a portable Qualified Signature Creation Device (QSCD) in compliance with requirements established in Annex II of EU Regulation 910/2014, and with the QcStatement extension set with the value "id-etsi-qcs-QcSSCD".

2.23. High-level Certificate for Public Servant with Pseudonym issued within Centralized QSCD

Qualified certificates issued to public servant with pseudonym that identify the subscriber as a Public Administration, and the signatory as the physical person within the service of that public administration..

The physical person is identified by their professional identification number. Identification of the public servant via first name, last name or Tax Identification Number is prohibited.

Comply with requirement established in Article 43 of Act 40/2015 of October 1st Public Sector Legal Regime for electronic signatures of personnel within the service of Public Administrations.

Qualified certificates due to the fact that they comply with requirements established in Annex I of the Regulation (EU) 910/2014.

Identified with the OID number: 1.3.6.1.4.1.13177.10.1.23.3

According to the spanish regulation, these certificates are identified with OID number: 2.16.724.1.3.5.4.1

Included in the Certification Policy for Electronic Signature Certificates.

The cryptographic keys of the signatory are created within a centralized Qualified Signature Creation Device (QSCD) in compliance with requirements established in Annex II of EU Regulation 910/2014, and with the QcStatement extension set with the value "id-etsi-qcs-QcSSCD".

2.24. Medium-level Certificate for Public Servant with Pseudonym issued within Other Devices

Qualified certificates issued to public servant with pseudonym that identify the subscriber as a Public Administration, and the signatory as the physical person within the service of that public administration.

The physical person is identified by their professional identification number. Identification of the public servant via first name, last name or Tax Identification Number is prohibited.

Comply with requirement established in Article 43 of Act 40/2015 of October 1st Public Sector Legal Regime for electronic signatures of personnel within the service of Public Administrations.

Qualified certificates due to the fact that they comply with requirements established in Annex I of the Regulation (UE) 910/2014.

Identified with the OID number: 1.3.6.1.4.1.13177.10.1.23.2

According to the spanish regulation, these certificates are identified with OID number: 2.16.724.1.3.5.4.2

Included in the Certification Policy for Electronic Signature Certificates.

These certificates shall not include a QcStatement extension with the value set as "id-etsi-qcs-QcSSCD"

2.25. High-level Certificate for Electronic Office

Issued to Public Administrations in accordance with stipulations of Article 38 of Act 40/2015 of October 1st Public Sector Legal Regime.

Comply with Annex IV of UE Regulation 910/2014 where requirements for qualified authentication certificates of web sites are specified.

Identified with the OID number: 1.3.6.1.4.1.13177.10.1.20.1

According to the spanish regulation, these certificates are identified with OID number: 2.16.724.1.3.5.5.1

Included in the Certification Policy for Website Authentication Certificates.

2.26. Medium-Level Certificate for Electronic Office

Issued to Public Administrations in accordance with stipulations of Article 38 of Act 40/2015 of October 1st Public Sector Legal Regime.

Comply with Annex IV of UE Regulation 910/2014 where requirements for qualified authentication certificates of web sites are specified.

Identified with the OID number: 1.3.6.1.4.1.13177.10.1.20.2

According to the spanish regulation, these certificates are identified with OID number: 2.16.724.1.3.5.5.2

Included in the Certification Policy for Website Authentication Certificates.

2.27. High-Level Body Seal Certificate issued within Portable QSCD

Generated in accordance with Annex III of EU Regulation 910/2014 where the requirements for such qualified certificates are specified.

Issued to Public Administrations, bodies or public law entities for use with devices, programs or applications maintained under the responsibility of the certificate subscriber or holder, in accordance with stipulations of Article 40 of Act 40/2015 October 1st of Public Sector Legal Regime

Used when signing on behalf of the body in systems for electronic signatures for automated administrative action.

Identified with OID number: 1.3.6.1.4.1.13177.10.1.21.1

According to the spanish regulation, these certificates are identified with OID number: 2.16.724.1.3.5.6.1

Included in the Certification Policy for Electronic Seal Certificates.

The cryptographic keys of the signatory are created within a portable Qualified Signature Creation Device (QSCD) in compliance with requirements established in Annex II of EU Regulation 910/2014, and with the QcStatement extension set with the value "id-etsi-qcs-QcSSCD".

2.28. High-Level Body Seal Certificate issued within Centralized QSCD

Generated in accordance with Annex III of EU Regulation 910/2014 where the requirements for such qualified certificates are specified.

Issued to Public Administrations, bodies or public law entities for use with devices, programs or applications maintained under the responsibility of the certificate subscriber or holder, in accordance with stipulations of Article 40 of Act 40/2015 October 1st of Public Sector Legal Regime

Used when signing on behalf of the body in systems for electronic signatures for automated administrative action.

Identified with OID number: 1.3.6.1.4.1.13177.10.1.21.3

According to the spanish regulation, these certificates are identified with OID number: 2.16.724.1.3.5.6.1

Included in the Certification Policy for Electronic Seal Certificates.

The cryptographic keys of the signatory are created within a centralized Qualified Signature Creation Device (QSCD) in compliance with requirements established in Annex II of EU Regulation 910/2014, and with the QcStatement extension set with the value "id-etsi-qcs-QcSSCD".

2.29. Medium-Level Body Seal Certificate issued within Other Devices

Generated in accordance with Annex III of EU Regulation 910/2014 where the requirements for such qualified certificates are specified.

Issued to Public Administrations, bodies or public law entities for use with devices, programs or applications maintained under the responsibility of the certificate subscriber or holder, in accordance with stipulations of Article 40 of Act 40/2015 October 1st of Public Sector Legal Regime

Used when signing on behalf of the body in systems for electronic signatures for automated administrative action.

Identified with the OID number 1.3.6.1.4.1.13177.10.1.21.2

According to the spanish regulation, these certificates are identified with OID number: 2.16.724.1.3.5.6.2

Included in the Certification Policy for Electronic Seal Certificates.

These certificates shall not include a QcStatement extension with the value set as "id-etsi-qcs-QcSSCD".

2.30. Certification Entity

All referred certificates are issued by FIRMAPROFESIONAL, as identified previously in this document.

3. Certificate Usage Limitations

3.1. Usage limitations for the Signatory

Signatory usage of certification service is bound by provisions for authorised use defined within the contract signed between FIRMAPROFESIONAL and the SUBSCRIBER, and subsequently set forth within the relevant section/s outlined on Signatory obligations.

Similarly the Signatory will undertake to use digital certification service in accordance with the instructions, manuals or procedures provided by FIRMAPROFESIONAL

The Signatory must comply with any law or regulation that may affect their right to use the cryptographic tools.

The Signatory may not adopt measures of inspections, alteration or reverse engineering of digital certification services of FIRMAPROFESIONAL without prior and express permission.

3.2. Usage Limitations for Verifiers

Certificates are to be used exclusively for their own functions and established purposes. Any other usage is not permitted.

Similarly, the certificates may only be used in accordance with applicable law.

End Entity certificates (a.k.a. leaf certificates), that is, those that are not Certification Authority certificates may not be used for signing requests for issuance, renewal, suspension or revocation of certificates, for signing public key certificates of any type, or for signing certificate revocation lists (CRL).

Certificates have not been designed for, and cannot be designated for use or resale within control equipment for dangerous uses, or for uses related to functioning of nuclear installations, navigational systems, aerial communications, arms control systems where failure could directly involve the loss of life, personal injuries or severe environmental damage.

These indicated limits must be taken into account when populating the various fields of certified profiles, as can be referred within the FIRMAPROFESIONAL web site (https://www.firmaprofesional.com).

Use of digital signatures within operations contradicting either this informative text or contracts with subscribers will be deemed unauthorised from a legal perspective, thereby releasing FIRMAPROFESIONAL from any liability arising from such usage that the signatory or any third party performs.

FIRMAPROFESIONAL will not have any access to data contained within transactions with the certificates. As a consequence of the technical impossibility of accessing the contents of a message, FIRMAPROFESIONAL is not able to issue any content validation, meaning that the subscriber, signatory or person/s responsible for custody will assume any liability arising from the contents linked to the use of a certificate.

Likewise, any liability that may arise from use beyond the limits and conditions established in this informative text or in the contracts with subscribers, as well as any other improper use described in this section or which may be interpreted as improper under current legislation, shall be attributable to the subscriber, the signatory or the person responsible for custody.

4. Subscriber Obligations

4.1. Key Generation

The subscriber authorizes FIRMAPROFESIONAL to generate the private and public keys (except for SSL certificates), in order to identify the electronic signatures of signatories, and request on their behalf the issuance of the certificate (indicating the type of certificate; for example, corporate certificate of a member of a Professional Association issued on portable QSCD).

4.2. Certificate Request

The subscriber undertakes to perform the requests of certificates in accordance with the proceeding provided by FIRMAPROFESIONAL in conformance with Certification Practices Statement (CPS) and operational documentation.

4.3. Obligations toward Information

It is the responsibility of the subscriber to ensure that all information included within a certificate request is accurate, complete for the certificate purpose, and up-to-date at all times

The subscriber must immediately inform FIRMAPROFESIONAL regarding:

- Any inaccuracy detected within an issued certificate
- Any changes in the information provided and/or registered for the issuance of the certificate
- The loss, robbery, theft or any other type of loss of control of the private key by the signatory

4.4. Protection Obligations

The subscriber undertakes to protect all information produced by their activity as the registry entity, except in the case of a personnel certificate which is not stipulated.

5. Signatory Obligations

5.1. Protection Obligations

The signatory undertakes to protect the personal identification code, the private keys and if necessary or any other technical medium delivered by FIRMAPROFESIONAL

In the case of loss or robbery of the private certificate key, or in cases where the signatory suspects that the private key has incurred a loss of reliability for any reason, the circumstances must be immediately communicated to FIRMAPROFESIONAL by the subscriber.

5.2. Obligations for Correct Use

The signatory must use the certification service (indicating the type of certificate for example, corporate certificate of a member of a Professional Association issued on portable QSCD provided by FIRMAPROFESIONAL) exclusively for the authorized uses contained within the CPS and in any other instruction, manual or procedure provided to the subscriber.

The signatory must comply with any law and regulation that may affect their right to use cryptographic tools.

The signatory may not adopt measures of inspection, alteration or decompiling of the provided services of digital certification.

The signatory shall recognize that:

a. Where they use any certificate, and while the certificate has not expired nor has been suspended or revoked, they accept the operational status of that certification.

b. Where they do not act as a certification entity, and therefore they undertake to not use private keys corresponding to the public keys contained in the certificates for the purpose of signing any certificate.

c. In the event that a private key were jeopardized its use is immediately and permanently suspended.

5.3. Prohibited transactions

The signatory undertakes not to use private keys, certificates or any other technical medium delivered by FIRMAPROFESIONAL, for the performance of any transaction prohibited by the applicable law.

Certificates have not been designed for, and cannot be designated for use or resale within control equipment for dangerous uses, or for uses related to functioning of nuclear installations, navigational systems, aerial communications, arms control systems where failure could directly involve the loss of life, personal injuries or severe environmental damage.

6. Verifier Obligations

6.1. Informed Decision

FIRMAPROFESIONAL will inform the verifier where it has access to sufficient information for making an informed decision when verifying a certificate and relying on the information contained within that certificate.

In addition, the verifier shall recognize that use of the Registry and the Certificate Revocation Lists (henceforth the ¨CRLs¨) of FIRMAPROFESIONAL are governed by the CPS of FIRMAPROFESIONAL, and they shall undertake to fulfill the technical, operational and security requirement described in the CPS.

6.2. Electronic Signatures Verification Requirements

Verification shall normally be executed automatically via software and in accordance with the DPC with the following requirements:

- Appropriate software to be used for the verification of digital signatures, with algorithms and the lengths of keys authorized in the certificate and/or execute any other cryptographic operation, and to establish the chain of certificates on which the electronic signature to be verified is based, since the electronic signature is verified using this chain of certificates.

- Ensure that the chain of identified certificates is the most appropriate for the electronic signature that is to be verified, since an electronic signature may be based on more than one chain of certificates and in such case it becomes the decision of the verifier to ensure that the most appropriate chain in used in order to verify it.

- To verify the revocation status of certificates in the chain using information provided by FIRMAPROFESIONAL Registry (via the CRLs for example) in order to determine the validity of all the certificates in the chain, since an electronic signature may only be deemed correctly verified if all certificates in the chain are correct and in current effect.

- To ensure that all the certificates in the chain authorize the use of private key by the certificate subscriber and the signatory, since it is possible that certain certificates will include usage limitations impeding trust in the electronic signature that is verified. Each certificate in the chain contains an indicator referring to the applicable use conditions that may be reviewed by the verifiers.

- Technically verify the signature of all certificates in the chain prior to trusting the certificate used by the signatory.

6.3. Trust a Non-Verified Certificate

If a verifier trusts a non-verified certificate they shall assume all risks arising from this action.

6.4. Verification Effect

By virtue of the correct verification of certificates in conformity with this informative text, the verifier may rely on the identification and if necessary the public key of the signatory within the limitation of the corresponding use, in order to create encrypted messages.

6.5. Correct use and prohibited actions

The verifier undertakes not to use any information regarding the status of certificates, or any other type of information having been provided by FIRMAPROFESIONAL, to perform any transaction prohibited by applicable law.

The verifier will not inspect, interfere or perform reverse engineering of the technical implementation of the public certification services of FIRMAPROFESIONAL without prior written consent.

In addition, the verifier must not intentionally jeopardize the security of public certification services of FIRMAPROFESIONAL.

Certificates have not been designed for, and cannot be designated for use or resale within control equipment for dangerous uses, or for uses related to functioning of nuclear installations, navigational systems, aerial communications, arms control systems where failure could directly involve the loss of life, personal injuries or severe environmental damage.

6.6. Indemnity Clause

A third party trusting in certificate/s undertakes not to hold FIRMAPROFESIONAL responsible for damages arising from any act or omission leading to liability, damage or loss, expense of any kind incurred (including judicial and legal representation costs), due to the publication and the use of certificate/s resulting in the following:

- Breach of obligations of the part of the third party trusting a certificate.
- Lack of verification to determine whether a certificate status is suspended or revoked
- Lack of verification of the full measures of assurance provided in the CPS or in other rules of application.

Certificates permit the encryption of documents, contents, messages of data under the exclusive liability of the signatory. FIRMAPROFESIONAL shall not be liable in any case for any loss of encrypted information that cannot be recovered.

7. FIRMAPROFESIONAL Obligations

7.1. Obligations regarding provision of Digital Certification Service

FIRMAPROFESIONAL undertakes to:

a. Issue, deliver, administer, suspend, revoke or renew certificates in accordance with instructions made by the subscriber, for all cases and reasons described in the CPS of FIRMAPROFESIONAL.

b. Execute the services with appropriate technical and material means, utilising personnel who fulfill the qualification and experience conditions established in the CPS.

c. Fulfill service quality levels in conformity with those established in the CPS, with regards to technical, operational and security aspects.

d. Notify the subscriber prior to the certificate expiration date to present the option to renew, or to inform regarding certificate suspension, lifting of a suspension or the revocation of certificates when such circumstances occur.

e. Communicate requesting third parties, the status of the certificates in accordance with the provisions established in the CPS regarding certificate verification services

7.2. Obligations regarding Register Verifications

FIRMAPROFESIONAL undertakes to issue certificates on the basis of data provided by the subscriber, while performing appropriate verifications regarding the identity of and other personal and supplementary information relating to the subscribers and ,where appropriate, also of the signatories

For such verifications FIRMAPROFESIONAL may deem necessary that documented justification (and/or any other document or relevant information relating to the subscriber and/or the signatory) be submitted by the signatory via the subscriber

In the event of FIRMAPROFESIONAL detecting errors in data to be included in certificates, or verifications of this data, it may perform changes deemed necessary prior to issuing the certificate, or alternatively suspending the issuance process while managing the corresponding incident with the subscriber. In the event that FIRMAPROFESIONAL corrects data without the prior management of the incident corresponding to the subscriber, it shall notify the subscriber of the data that is finally certified.

FIRMAPROFESIONAL reserves the right not to issue a certificate when it deems that documented justification is insufficient for the correct identification and authentication of the subscriber and/or the signatory.

Previous obligations shall be suspended in cases where the subscriber acts as a registry authority and maintains technical functions corresponding to key generation, certificate issuance and the recording of signature devices.

7.3. Retention Periods

FIRMAPROFESIONAL retains all registries corresponding to the issuance and renewal requests of certificates for at least 15 years, from the expiration of the certificate or the end of the service provided.

FIRMAPROFESIONAL stores log information during a period of between 1 and 15 years depending on the type of information registered.