Firmaprofesional Informative TEXT (PDS) of Personal, Corporate, Public Administration, Body or Public Law Entity certificates.

Version:	170220
Classification:	**Public**
Publication Date:	**20/02/2017**

ATTENTION: The original copy in effect of this document is found in electronic format at https://www.firmaprofesional.com/cps/pds_en.pdf

Past Versions

Version	Section and Changes
170220	Initial Version

Table of Contents

INFORMATIVE TEXTS

APPLICABLE TO

PERSONAL, CORPORATE, PUBLIC ADMINISTRATION, BODY OR PUBLIC LAW ENTITY CERTIFICATES

This document contains the essential information to know in regard to the certification service of the FIRMAPROFESIONAL Certification Entity.

1. Contact Information

1.1. Responsible Organization

The Certification Entity FIRMAPROFESIONAL, hereinafter “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.
Edificio ESADECREAPOLIS Avda. Torre Blanca, 57. Local M2.
08173 Sant Cugat del Vallés
Tel: (+34) 902 361 639

2. Types and purposes of certificates

2.1. Personal Certificate

They are qualified certificates of a physical person that identify a subscriber and a signer as the same physical person who needs to carry out relations with Public Administrations and other institutions.

They are qualified certificates because they comply with the requisites established in Exhibit I of Regulation (EU) 910/2014.

They are identified with the OID number: 1.3.6.1.4.1.13177.10.1.40.2 and other institutions.

These certificates will not include the enabled extension QcStatement with value “id-etsi-qcs-QcSSCD”.

2.2. Corporate Certificate of a Member of Professional Organization Issued on a Portable QSCD

They are qualified certificates of a physical person which identify a subscriber as a Professional Organization and the signer as a professional who is a member of such Professional Organization.

They are **qualified** certificates because they comply with the requisites established in Exhibit I of Regulation (EU) 910/2014)

They are identified with the OID number: 1.3.6.1.4.1.13177.10.1.1.1

The cryptographic keys of the signer have been created on a portable Qualified Signature Creation Device (QSCD) in compliance with the requisites established in Article 24 of Act 59/2003 of December 19 on Electronic Signatures and in Exhibit II of EU Regulation 910/2014 by which they shall have enabled the QcStatement extension with the value, “id-etsi-qcs-QcSSCD”.

2.3. Corporate Certificate of a Member of a Professional Organization Issued on a Centralized QSCD

They are qualified certificates of a physical person that identify a subscriber as the Professional Organization and the signer as a Member of said Professional Organization.

They are qualified certificates because they fulfill the requisites established in Exhibit I of Regulation (EU) 910/2014.

They are identified with the OID number: 1.3.6.1.4.1.13177.10.1.1.3

The cryptographic keys of the signer have been created on a centralized Qualified Signature Creation Device (QSCD) in compliance with the requisites established in Article 24 of Act 59/2003 of December 19 on Electronic Signatures and Exhibit II of EU Regulation 910/2014 by which they shall have enabled the QcStatement extension with value“id-etsi-qcs-QcSSCD”.

2.4. Corporate Certificate of a Member of a Professional Organization Issued on Software

They are qualified certificates of physical persons that identify the subscriber as a Professional Organization and the signer as a Member of said Professional Organization.

They are qualified certificates because they fulfill requisites established in Exhibit I of the Regulation. (EU) 910/2014.

These certificates shall not include the enabled extension QcStatement with value “id-etsi-qcs-QcSSCD”. Regulation (EU) 910/2014.

2.5. Corporate Certificate of a Physical Person Issued on a Portable QSCD

They are qualified certificates of a physical person that identifies a subscriber as a Corporation and the signer as a physical person linked to that Corporation, whether they are an employee, associate, collaborator, client, supplier or have another type of

relationship. They are qualified certificates because they comply with the requisites established in Exhibit I of Regulation (EU) 910/2014

They are identified with the OID number: 1.3.6.1.4.1.13177.10.1.2.1

They cryptographic keys of the signer have been created on a portable Qualified Signature Creation Device (QSCD) in compliance with the requisites established in Article 24 of the Act 59/2003 of December 19 on Electronic Signatures and in Exhibit II of EU Regulation 910/2014 by which they will have enabled the QcStatement extension with the value “id-etsi-qcs-QcSSCD”.

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

They are qualified certificates of a physical person that identify a subscriber as a Corporation and the signer as a physical person related to that Corporation whether they are an employee, associate, collaborator, client, supplier or have another type of relationship.

They are qualified certificates because they comply with the requisites established in Exhibit I of the Regulation (UE) 910/2014.

They are identified with OID number: 1.3.6.1.4.1.13177.10.1.2.3

The cryptographic keys of the signer have been created on a centralized Qualified Signature Creation Device (QSCD) in compliance with the requisites established in Article 24 of Act 59/2003 of December 19 on Electronic Signatures and in Exhibit II of EU Regulation 910/2014 which will have enabled the QcStatement extension with the value, “id-etsi-qcs-QcSSCD”

2.7. Corporate Certificate of a Physical Person Issued on Software

They are qualified certificates of a physical person that identify the subscriber as a Corporation and the signer as a physical person linked to that Corporation whether they are an employee, associate, collaborator, client, supplier or have another type of relationship.

They are qualified certificates because they comply with the requisites established in

Exhibit I of Regulation (EU) 910/2014)

They are identified with the OID number: 1.3.6.1.4.1.13177.10.1..2

These certificates shall not include the enabled QcStatement extension with value "id-etsi-qcs-QcSSCD¨.

2.8. Corporate Certificate of a Legal Representative on a Portable QSCD

They are qualified certificates of a physical person that identify a subscriber as a Corporation and the signer as a legal representative of said Corporation.

They are qualified certificates because they comply with the requisites established in Exhibit I of Regulation (UE) 910/2014.

They are identified with the OID number: 1.3.6.1.4.1.13177.10.1.11.1

They cryptographic keys of the signer have been created on a portable Qualified Signature Creation Device (QSCD) in compliance with the requisites established in Article 24 of Act 59/2003 of December 19 on Electronic Signatures and in Exhibit II of EU Regulation 910/2014 which shall have enabled the QcStatement extension with the value "id-etsi-qcs-QcSSCD".

2.9. Corporate Certificate of a Legal Representative on a Centralized QSCD

They are qualified certificates of a physical person that identifies a subscriber as a Corporation and the signer as a legal representative of said Corporation.

They are qualified certificates because they comply with the requisites established in Exhibit I of the Regulation (EU) 910/2014.

They are identified with the OID number: 1.3.6.1.4.1.13177.10.1.11.3

The cryptographic keys of the signer have been created on a centralized Qualified Signature Creation Device (QSCD) in compliance with the requisites established in Article 24 of Act 59/2003 of December 19 on Electronic Signatures and in Exhibit II of

EU Regulation 910/2014 which shall have enabled the QcStatement extension with value ¨id-etsi-qcs-QcSSCD¨.

2.10. Corporate Certificate of a Legal Representative on Software

They are qualified certificates of a physical person that identify the subscriber as a Corporation and the signer as a legal representative of said Corporation.

They are qualified certificates because they comply with the requisites established in Exhibit II of Regulation (EC) 910/2014.

They are identified with OID number: 1.3.6.1.4.1.13177.10.1.11.2

These certificates shall not include the enabled extension QcStatement with “id-etsi-qcs-QcSSCD¨ value.

2.11. Corporate Certificate of a Voluntary Legal Representative on a Portable QSCD

They are qualified certificates of a physical person that identify a subscriber as a Corporation and the signer as a voluntary representative with specific general powers of said Corporation in order to act before public administrations.

They are qualified certificates because they fulfil the requisites established in Exhibit I of the Regulation (EU) 910/2014.

They are identified with the OID number: 1.3.6.1.4.1.13177.10.1.12.1

The cryptographic keys of the signer have been created on a portable Qualified Signature Creation Device (QSCD) in compliance with the established in Article 24 of Act 59/2003 of December 19 on Electronic Signatures and in Exhibit II of EU Regulation 910/2014 which shall have enabled the QcStatement extension with value “id-etsi-qcs-QcSSCD”.

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

They are qualified certificates of a physical person that identify a subscriber as a Corporation and the signer as a voluntary representative with specific general powers of attorney of said Corporation in order to act before public administrations.

They are qualified certificates because they comply with the requisites established in Exhibit I of Regulation (EU) 910/2014.

They are identified with OID number: 1.3.6.1.4.1.13177.10.1.12.3

The cryptographic keys of the signer have been created on a centralized Qualified Signature Creation Device (QSCD) in compliance with the requisites established in Article 24 of Act 59/2003 of December 19 on Electronic Signatures and in Exhibit II of EU Regulation 910/2014 which shall have enabled the QcStatement extension with value “id-etsi-qcs-QcSSCD”

2.13. Corporate Certificate of a Voluntary Legal Representative on Software

They are qualified certificates of a physical person that identify a subscriber as a Corporation and a signer as a voluntary representative with specific general powers of said Corporation in order to act before the public administrations.

They are qualified certificates because they comply with the requisites established in Exhibit I of Regulation (EU) 910/2014.

They are identified with the OID number: 1.3.6.1.4.1.13177.10.1.12.2

These certificates shall not include enabled the QcStatement extension with value “id-etsi-qcs-QcSSCD”.

2.14. Corporate Certificate with Company Seal

They are electronic certificates issued to legal persons in conformity 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.

They are qualified certificates because they comply with the requisites established in Exhibit III of the Regulation (EU) 910/2014.
They are identified with the OID number: 1.3.6.1.4.1.13177.10.1.10.2

These certificates shall not include enabled the QcStatement extension with the value “id-etsi-qcs-QcSSCD”.

2.15. SSL EV-256 Certificate

They are qualified certificates used in order to authenticate a Web server on the part of the navigators by means of the use of the HTTPS protocol with extended validation guarantees of the entity which owns the server.

They are qualified certificates because they comply with the requisites established in Exhibit IV of EU Regulation 910/2014.

They are identified with OID number: 1.3.6.1.4.1.13177.10.1.3.10

2.16. TSA/VA Certificate

They are qualified certificates that permit signing digital evidence such as the Time Stamping Authority (TSA) or the Validation Authority (VA).

They are qualified certificates because they comply with the requisites of Articles 41 and 42 of EU Regulation EU 910/2014.

They are identified with the OID number: 1.3.6.1.4.1.13177 20.0.1 of October 1 on the Legal Regime of the Public Sector for electronic signatures of personnel at the service of Public Administrations.

They are qualified certificates because they comply with the requisites established in Exhibit 1 of Regulation (EU) 910/2014.

They are identified with the OID number: 1.3.6.1.4.1.13177.10.1.22.1

They are identified with the Spanish policy with OID number: 2.16.724.1.3.5.7.1

The cryptographic keys of the signer have been created on a Portable Qualified Signature Creation Device (QSCD) in compliance with the requisites established in Article 24 of Act 59/2003 of December 19 on Electronic Signatures and in Exhibit II of EU Regulation 910/2014 which shall have enabled the QcStatement extension with the value “id-etsi-qcs-QcSSCD”.

2.17. Certificate of Public Employee with High-Level on a Portable QSCD

They are qualified certificates of a public employee that identify the subscriber as a Public Administration and the signer as a physical person in the service of that public administration.

They are certificates that follow the requisites established in Article 43 of Act 40/2015 of October 1 on the Legal Regime of the Public Sector for electronic signatures of personnel in the service of Public Administrations.

They are qualified certificates because they comply with the requisites established in Exhibit 1 of the Regulation (EU) 910/2014.

They are identified with the OID number: 1.3.6.1.4.1.13177.10.1.22.3

They are identified with the Spanish policy with OID number: 2.16.724.1.3.5.7.1

The cryptographic keys of the signer have been created on a centralized Qualified Signature Creation Device (QSCD) in compliance with the requisites established in Article 24 of Act 59/2003 of December 19 on Electronic Signatures and in Exhibit II of EU Regulation 910/2014 which will have enabled the QcStatement extension with value “id-etsi-qcs-QcSSCD”.

2.18. Certificate of Public Employee with High-Level on a Centralized QSCD

They are qualified certificates of a public employee that identify a subscriber as a Public Administration and the signer as a physical person in the service of that public

administration.

They are certificates that follow the requisites established in Article 43 of Act 40/2015 of October 1 on the Legal Regime of the Public Sector for electronic signatures of personnel at the service of Public Administrations.

They are qualified certificates because they fulfill the requisites established in Exhibit I of the Regulation (EC) 910/2014.

They are identified with OID number: 1.3.6.1.4.1.13177.10.1.22.3

They are identified with the Spanish policy with OID number 2.16.724.1.3.5.7.1

The cryptographic keys of the signer have been created on a centralized Qualified Signature Creation Device (QSCD) in compliance with the requisites established in Article 24 of Act 59/2003 of December 19 on Electronic Signatures and Exhibit II of EU Regulation 910/2014 for which they will have enabled the QcStatement extension with value “id-etsi-qcs-QcSSCD”.

2.19. Certificate of Public Employee with Medium-Level

They are qualified certificates of a public employee that identifies a subscriber as a Public Administration and the signer as a physical person at the service of that public administration.

They are certificates that follow the requisites established in Article 43 of Act 40/2015 of October 1 on the Legal Regime of the Public Sector for electronic signatures of personnel at the service of the Public Administrations.

They are identified with OID number: 1.3.6.1.4.1.13177.10.1.22.2

They are identified with the Spanish policy with number of OID: 2.16.724.1.3.5.7.2

These certificates **shall not include** disabled the extension QcStatement with value “id-etsi-qcs-QcSSCD”.

2.20. Certificate of an Anonymous Public Employee with High-Level on a Portable QSCD

They are qualified certificates of an anonymous public employee that identify a subscriber as a Public Administration and the signer as a physical person at the service of that public administration.

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

They are certificates that follow the requisites established in Article 43 of Act 40/2015 of October 1 on the Legal Regime of the Public Sector for electronic signatures of personnel at the service of the Public Administrations.

They are qualified certificates because they comply with the requisites established in Exhibit I of Regulation (EU) 910/2014.

They are identified with the OID number: 1.3.6.1.4.1.13177.10.1.23.1

They are identified with the Spanish Policy with the OID number: 2.16.724.1.3.5.4.1

The cryptographic keys of the signer have been created on a Qualified Signature Creation Device (QSCD) in compliance with the requisites established in Article 24 of Act 59/2003 of December 19 on Electronic Signatures and in Exhibit II of EU Regulation 910/2014 which shall have enabled the QcStatement extension with the value “id-etsi-qcs-QcSSCD”.

2.21. Certificate of an Anonymous Public Employee with High-Level on a Centralized QSCD

They are qualified certificates of an anonymous public employee that identify a subscriber as a Public Administration and the signer as a physical person at the service of that public administration.

The physical person is identified by their professional identification. Indicating the name, last name or Tax Identification Number of a public employee is prohibited.

They are certificates that follow the requisites established in Article 43 of Act 40/2015

of October 1 on the Legal Regime of the Public Sector for the electronic signing of the personnel at the service of Public Administrations.

They are qualified certificates because they comply with the requisites established in Exhibit I of the Regulation (EU) 910/2014.

They are identified with the OID number: 1.3.6.1.4.1.13177.10.1.23.3

They are identified with the Spanish Policy with the OID number: 2.16.724.1.3.5.4.1

The cryptographic keys of the signer have been created on a centralized Qualified Signature Creation Device (QSCD) in compliance with the requisites established in Article 24 of Act 59/2003 of December 19 on Electronic Signatures and in Exhibit II of EU Regulation 910/2014 which shall have enabled the QcStatement extension with the value “id-etsi-qcs-QcSSCD”.

2.22. Certificate of an Anonymous Public Employee with Middle-Level

They are qualified certificates of an anonymous public employee that identify a subscriber as a Public Administration and the signer as a physical person at the service of that public administration.

The physical person is identified by their professional identification number. Indicating the name, last name or Tax Identification Number of a public employee is prohibited.
They are certificates that follow the requisites established in Article 43 of Act 40/2015 of October 1 on the Legal Regime of the Public Sector for the electronic signatures of personnel at the service of the Public Administrations.

They are qualified certificates because they comply with the requisites established in Exhibit I of the Regulation (UE) 910/2014.

They are identified with the OID number: 1.3.6.1.4.1.13177.10.1.23.2

They are identified with the Spanish policy with the OID numer: 2.16.724.1.3.5.4.2

These certificates **shall not include** enabled the QcStatement extension with value “id-etsi-qcs-QcSSCD”.

2.23. Certificate of an Electronic Office with High-Level

The Certificates of High-Level Electronic Office are certificates issued to Public Administrations in accordance with the indications of Article 38 of Act 40/2015 of October 1 on the Legal Regime of the Public Sector.

They are in accordance with Exhibit IV of UE Regulation 910/2014 that specifies the requisites for the qualified authentication certificates of web sites.

They are identified with the OID number: 1.3.6.1.4.1.13177.10.1.20.1

They are identified with the Spanish Policy with the OID number: 2.16.724.1.3.5.5.1

2.24. Certificate of an Electronic Office with Medium-Level

The Medium-Level Certificates of an Electronic Office in accordance with the indications of Article 38 of Act 40/2015 of October 1 on the Legal Regime of the Public Sector.

They are in accordance with Exhibit IV of EU Regulation 910/2014 that specify the requisites for qualified authentication certificates of web sites.

They are identified with the OID number: 1.3.6.1.4.1.13177.10.1.20.2

They are identified with the Spanish policy with the OID number: 2.16.724.1.3.5.5.2

2.25. Seal Certificate of a Body with High-Level

The Seal Certificates of a High-Level Public Administration, Body or Public-Law Entity are in accordance with Exhibit III of EU Regulation 910/2014 that specifies the requisites for the qualified electronic seal certificates.

They are issued to Public Administrations, bodies or public law entities for computer devices, programs or applications under the responsibility of a subscriber or a holder of the certificate in accordance with the indications of Article 40 of Act 40/2015 of October 1 on the Legal Regime of the Public Sector.

Their purpose is the ability to sign on behalf of the body in systems for electronic signatures for automated administrative action.

They are identified with OID number: 1.3.6.1.4.1.13177.10.1.21.1

They are identified with the Spanish Policy with the OID number 2.16.724.1.3.5.6.1

2.26. Seal Certificate of a Body with Medium-Level

The Seal Certificates of a Medium-Level Public Administration, Body or Public Law Entity are in accordance with Exhibit III of EU Regulation 910/2014 that specifies the requisites for the **qualified** electronic seal **certificates**.

They are issued to Public Administrations, bodies or public law entities for computer devices, programs or applications under the responsibility of the subscriber or holder of the certificate in accordance with the indications of Article 40 of Act 40/2015 of October 1 on the Legal Regime of the Public Sector.

Their purpose is the ability to sign on behalf of the body in electronic signature systems for automated administrative action. They are identified with the OID number 1.3.6.1.4.1.13177.10.1.21.2. They are identified with the Spanish policy with the OID number 2.16.724.1.3.5.6.2

2.27. Entity Issuing Certification

The indicated certificates are issued by FIRMAPROFESIONAL, identified by means of the previously indicated data.

3. Limits on Certificate Use

3.1. Limits on Use Pertaining to Signers

The signer must use the certification service of the certificates supplied by FIRMAPROFESIONAL exclusively for the uses authorized in the contract signed between FIRMAPROFESIONAL and the SUBSCRIBER and that are subsequently set forth (section on obligations of the signers).

Likewise, the signer undertakes to use the digital certification service in accordance with the instructions, manuals or procedures provided by FIRMAPROFESIONAL.
The signer must comply with any law or regulation that may affect their right to use the cryptographic tools that they use.

The signer cannot adopt measures of inspections, alteration or reverse engineering of the digital certification services of FIRMAPROFESIONAL without express prior permission.

3.2. Limits Pertaining to Verifiers

The certificates are to be used for their own functions and established purposes without being able to be used in other functions and for other purposes.

Similarly, the certificates may only be used in accordance with the applicable law, especially taking into account the import and export restrictions in existence at any time.

The certificates may not be used for signing requests for issuance, renewal, suspension or revocation of certificates nor for signing public key certificates of any type nor signing certificate revocation lists (CRL).

The certificates have not been designed, cannot be designated and their use or resale as control equipment for dangerous uses and for uses that require actions such as the functioning of nuclear installations, navigational systems, aerial communications, arms control systems where a breakdown could directly involve the loss of life, personal injuries or severe environmental damage.

The indicated limits must be taken into account in the various fields of certified profiles, which can be seen on the FIRMAPROFESIONAL web site (https://www.firmaprofesional.com).

The use of the digital signatures in operations that contradict this informative text or the contracts with subscribers is to be deemed undue use for purposes of appropriate legal effects, thereby releasing FIRMAPROFESIONAL in function of the legislation in effect from any liability for the undue use of the certificates that the signer or any third party performs.

FIRMAPROFESIONAL does not have any access to data over which the use of a certificate may apply. Therefore, and as a consequence of this technical impossibility of accessing the contents of the message, it is not possible on the part of FIRMAPROFESIONAL to issue any valuation on said contents, assuming therefore the subscriber, the signer or the person responsible for safe-keeping any liability arising from the contents linked to the use of a certificate.

Likewise, any liability that may arise from the use thereof beyond the limits and use conditions set forth in this informative text or in the contracts with subscribers as well as any other undue use thereof arising from this section or that may be interpreted as such in function of the legislation in effect shall be attributable to the subscriber, the signer or the person responsible for the safe-keeping.

4. Obligations of Subscribers

4.1. Generation of Keys

The subscriber authorizes FIRMAPROFESIONAL to generate the keys, private and public in order to identify the electronic signatures of the signers and request on their behalf the issuance of the certificate (indicate the type of certificate for example, corporate certificate of a member of a Professional Organization issued on the portable QSCD).

4.2. Request of Certificates

The subscriber undertakes to perform the requests of certificates in accordance with the proceeding and if necessary, the technical components supplied by FIRMAPROFESIONAL in conformity with that which is established in the Certification Practice Statement (CPS) and in the FIRMAPROFESIONAL documentation of operations.

4.3. Information Obligations

The responsibility of the subscriber is for all the information included in the certificate request to be exact, complete for the purpose of the certificate and be up-to-date at all times.

The subscriber must immediately inform FIRMAPROFESIONAL:

- Of any inexactness detected in the certificate once it has been issued.
- Of the changes that occur in the information provided and/or registered for the issuance of the certificate.
- Of the loss, robbery, theft or any other type of loss of control of the private key by the signer.

4.4. Safeguarding Obligations

The subscriber undertakes to safeguard all the information that it produces in their activity as the registry entity except in the case of a personnel certificate since it is not found stipulated.

5. Obligations of the Signers

5.1. Safeguarding Obligations

The signer undertakes to safekeep the personal identification code or any other technical support delivered by FIRMAPROFESIONAL, the private keys and if necessary the property specifications of FIRMAPROFESIONAL that are provided to them. The signer is obligated to safekeep the personal identification code (PIN).
In the case of loss or robbery of the private certificate key or in the case that the signer suspected that the private key has incurred a loss of reliability for any reason, said circumstances must be immediately communicated to FIRMAPROFESIONAL by means of the subscriber.

5.2. Obligations of Correct Use

The signer must use the certification service of certificates (indicate the type of certificate for example, corporate certificate of a member of a Professional Organization issued on a portable QSCD provided by FIRMAPROFESIONAL, exclusively for the authorized uses in the CPS and in any other instruction, manual or proceeding provided to the subscriber.

The signer has to comply with any law and regulation that may affect their right to use the cryptographic tools used.

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

The signer shall recognize:

a) Whereas when they use any certificate and while the certificate has not expired nor has been suspended or revoked they shall have to accept said certification and it shall be operative.

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

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

5.3. Prohibited transactions

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

The digital certification services provided by FIRMAPROFESIONAL have not been designed nor permit their use or resale as control equipment of dangerous situations or for uses that require fail-proof actions such as the operation of nuclear installations, navigational system or aerial communications, air-trafficking control systems, systems for weapons control in which an error could directly cause the loss of life, physical injuries or serious environmental damage.

6. Obligations of Verifiers

6.1. Informed Decision

FIRMAPROFESIONAL informs the verifier that it has access to sufficient information for making an informed decision when verifying a certificate and relying on the information contained in said certificate.

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

6.2. Verification Requisites of Electronic Signatures

The verification shall normally be executed automatically by the verifier software and in any case in accordance with the DPC with the following requisites:

- It is necessary to use the appropriate software for the verification of a digital signature with the 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.

- It is necessary to ensure that the chain of identified certificates is the most adequate for the electronic signature that is to be verified since an electronic signature may be based on more than a chain of certificates and it is the decision of the verifier to ensure the use of the most adequate chain in order to verify it.

- It is necessary to verify the state of revocation of the certificates of the chain with the information provided the FIRMAPROFESIONAL Registry (with the CRLs for example) in order to determine the validity of all the certificates of the chain of certificates, since an electronic signature may only be deemed correctly verified if each and every one of the certificates of the chain are correct and in effect.

- It is necessary to ensure that all the certificates of the chain authorize the use of the private key by the certificate subscriber and the signer since there is a possibility that some of the certificates include use limits that impede relying on the electronic signature that is verified. Each certificate of the chain has an indicator that makes reference to the applicable use conditions for their review by the verifiers.

- It is necessary to technically verify the signature of all the certificates of the chain prior to relying on the certificate used by the signer.

6.3. Reliability of a Non-Verified Certificate

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

6.4. Verification Effect

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

6.5. Correct use and prohibited activities

The verifier undertakes to not use any type of information on the state of the certificates or any other type that has been provided by FIRMAPROFESIONAL in the performance of any transaction prohibited by the law applicable to said transaction.

The verifier undertakes to 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 is obligated to not intentionally jeopardize the security of the public certification services of FIRMAPROFESIONAL.

The digital certification services, provided by FIRMAPROFESIONAL, have not been designed nor permit the use or resale, as equipment for controlling dangerous situations or for uses that require fail-proof such as the operation of nuclear installations, navigational systems or aerial communication, air trafficking control systems or systems for arms control where an error could cause the loss of life, physical injuries or serious environmental damage.

6.6. Indemnity Clause

A third party that relies on the certificate undertakes to hold FIRMAPROFESIONAL harmless for any damages arising from any act or omission that leads to liability, damage or loss, expense of any type including judicial expenses and those of legal

representation in which it could incur due to the publication and the use of the certificate when any of the following causes concur:

- Breach of the obligations of the third party that relies on the certificate.
- Reckless reliance on a certificate under the circumstances.
- Lack of verification of the state of a certificate in order to determine that it is not suspended or revoked.
- Lack of verification of the totality of the measures of assurance provided in the CPS or in the other rules of application.

The indicated certificate permits the encryption of documents, contents, messages of data under the exclusive liability of the signer. FIRMAPROFESIONAL shall not be liable in any case for any loss of encrypted information that cannot be recovered.

7. FIRMAPROFESIONAL Obligations

7.1. In regard to providing the service of digital certification

FIRMAPROFESIONAL undertakes to:

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

b) Execute the services with adequate technical and material means and with personnel who fulfill the conditions of qualification and experience established in the CPS.

c) Fulfill the levels of service quality in conformity with that which is established in the CPS, insofar as the technical, operational and security aspects.

d) Notify the subscriber prior to the expiration date of the certificates of the option to renew them as well as the suspension, lifting of this suspension or the revocation of the certificates when said circumstances occur.

e) Communicate to third parties who request, the state of the certificates in accordance with that which is established in the CPS for the various verification services of the certificates.

7.2. In regard to Registry Verifications

FIRMAPROFESIONAL undertakes to issue certificates on the basis of the data provided by the subscriber for which it shall perform the verifications that it deems appropriate with respect to the identity and other personal and supplementary information of the subscribers and when it is appropriate, of the signers.

These verifications may include the documentary justification contributed by the signer by means of the subscriber if FIRMAPROFESIONAL deems it necessary and any other document or relevant information provided by the subscriber and/or the signer.

In the event that FIRMAPROFESIONAL detects errors in the data that must be included in the certificates or that justifies this data, it may perform the changes that it deems necessary prior to issuing the certificate or suspending the issuance process and managing the corresponding incident with the subscriber. In the event that FIRMAPROFESIONAL corrected the 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 to not issue the certificate when it deems that the documentary justification is insufficient for the correct identification and authentication of the subscriber and/or the signer.

The previous obligations shall be suspended in the cases in which the subscriber acts as a registry authority and disposes of the technical elements corresponding to the generation of keys, issuance of certificates and the recording of signature devices.

7.3. Conservation Periods

FIRMAPROFESIONAL saves the registries corresponding to the issuance and renewal requests of certificates for at least 15 years.

FIRMAPROFESIONAL stores the information of the logs during a period of between 1 and 15 years in function of the type of information registered.

8. Limited Guarantees and Rejection of Guarantees

8.1. FIRMAPROFESIONAL Guarantee for Digital Certification Services

FIRMAPROFESIONAL guarantees the subscriber

- That there are not any factual errors in the information contained in the certificates known or performed by the Certification Entity.
- That there are not any factual errors in the information contained in the certificates due to the lack of due diligence in the management of the certificate request or in the creation thereof.
- That the certificates comply with all the material requisites established in the CPS.
- That the renewal services and the use of the depository comply with all the material requisites established in the CPS.
- FIRMAPROFESIONAL guarantees the third party that relies on the certificate.
- That the information contained in included by reference in the certificate is correct except when otherwise indicated.
- In the event of certificates published in the depository that the certificate has been issued to the subscriber and the signer identified therein and that the certificate has been accepted.
- That in the approval of the certificate request and the certificate issuance all the material requisites established in the CPS have been fulfilled.
- The speed and security in the provision of services in particular, the services of renewal and deposit.
- In addition FIRMAPROFESIONAL guarantees the subscriber and the third party that trust the certificate.
- That the certificate contains that information that a recognized/qualified certificate must contain in accordance with Article 11 of Act 59/2003 of December 19 and Exhibit I of the Regulation (EU) No 910/2014 of the European Parliament and Council of July 23,, 2014 related to the electronic identification and trusted services for electronic transactions in the domestic market and for which Directive 1999/93/EC is repealed.

- That in the event that it generates private keys of the subscriber or if the case, the physical person identified in the certificate, their confidentiality is maintained during the process.
- The liability of the Certification Entity within the limits that are established. Under no circumstances shall FIRMAPROFESIONAL be liable for fortuitous events or in the event of force majeure.

8.2. Exclusion of the guarantee

FIRMAPROFESIONAL hereby rejects all other guarantees other than the previous that are not legally enforceable.

Specifically, FIRMAPROFESIONAL does not guarantee any software used by any person in order to sign, verify signature, code, decode or use any other digital certificate issued by FIRMAPROFESIONAL except in the cases there is otherwise a written statement.

9. Applicable Agreements and CPS

9.1. Applicable Agreements

The agreements applicable to the certificates are as follows:

- Contract for certification services that regulates the relationship between FIRMAPROFESIONAL and the company, subscriber of the certificates or in the case of personal certificates between FIRMAPROFESIONAL and the subscriber of the certificate.
- General Conditions of the services included in the text revealing the certificate or the PDS.
- CPS that regulates the issuance and use of the certificates.
- Certification Policy (CP) of each one of the certificates.

9.2. CPS

The certification services of FIRMAPROFESIONAL are regulated technically and operationally by the CPS of FIRMAPROFESIONAL, by its subsequent actions as well as by supplementary documentation.

The CPS and the documentation on the operations are modified periodically in the Registry and may be consulted on the Internet Page. https://www.firmaprofesional.com.

10. Rules for Trust of Long Time Signatures

Point b.2 of Article 18 of Act 59/2003 of December 19 on electronic signatures refers to the obligation of certification entities to inform those applying for the mechanisms in order to guarantee the reliability of the electronic signature of a document over time.

FIRMAPROFESIONAL informs those certificate applicants that it does not offer a service that guarantees the reliability of the electronic signature of a document over time.

FIRMAPROFESIONAL recommends that for the reliability of the electronic signature of a document over time, the use of the standards indicated in section 7.3 (rules for trust of long-time signatures) of the Application Guide on the Technical Regulation of Interoperability ¨Policy on Electronic Signatures and Administration Certificates¨.

The general consideration for the rules for trust of long-time signatures are set forth in sub-section IV.3 of the NTI on electronic signatures.

11. Confidentiality Policy

FIRMAPROFESIONAL cannot reveal nor be obligated to reveal any confidential information referring to the certificates without a specific prior request that arises from:

a) The person with respect to which FIRMAPROFESIONAL has the duty to keep information confidential or

b) A judicial or administrative order or one from any other provided for in the legislation in effect.

Nevertheless, the subscriber accepts that certain information, personal or otherwise,

provided in the application for certificates whether included in their certificates or in the mechanism for verification of the state of the certificates and the mentioned information does not have a confidential nature by legal imperative.

FIRMAPROFESIONAL does not transfer to any person the data delivered specifically for the provision of the certification service.

12. Privacy Policy

FIRMAPROFESIONAL disposes of a privacy policy in Section 9.4 of the CPS and a specific privacy regulation in relation to the registry process, the confidentiality of the registry, the protection of Access to personal information and the user consent.

Likewise, it is contemplated that the verifying accreditation documentation regarding the approval of the request must be conserved and duly registered and with the security guarantees and integrity during a period of 15 years from the expiration of the certificate even in the case of an early loss of effectiveness due to revocation.

13. Refund Policy

FIRMAPROFESIONAL shall not refund the cost of the certification cost under any circumstances.

14. Applicable Law and Forum

The relations with FIRMAPROFESIONAL shall be governed by Spanish Law and specifically by the Regulation (EU) No 910/2014 of the European Parliament and the Council of July 23 2014 related to electronic identification and the trusted services for the electronic transactions in the domestic market and by which Directive 1999/93/EC, Act 59/2003 of December 19 on electronic signatures is repealed as well as by the applicable civil and mercantile legislation.

The competent jurisdiction is that which is indicated in Act 1/2000 of January 7 on Civil Procedures.

15. Accreditations and Quality Seals

Without stipulations.

16. Links with the list of suppliers

http://www.minetur.gob.es/telecomunicaciones/es-es/servicios/firmaelectronica/paginas/prestadores.aspx

17. Severability of the clauses, survivorship, complete agreement and notices.

The clauses of this informative text are independent from one another the reason for which if any of the clauses were deemed invalid or inapplicable the remainder of the clauses of the PDS shall continue being applicable except with express agreement otherwise of the parties.

The requisites contained in the corresponding sections of Obligations, Liability, Auditing of conformity and Confidentiality of the Certification Practice Statement of FIRMAPROFESIONAL shall continue in effect after the termination of the service.

This text contains the complete will and all the agreements between the parties.

The interested parties may provide notice by means of communication at the address provided in the contact information of this PDS or by means of sending an e-mail to the Firmaprofesional e-mail addresss cumplimiento@firmaprofesional.com