PKI Disclosure Statement (PDS) - Electronic Signature and Authentication CertificatesPKI Disclosure Statement (PDS) - Electronic Signature and Authentication Certificates



PKI Disclosure Statement (PDS)

UANATACA, S.A.
Avenida Meridiana 350, 3ª planta 08027 Barcelona (España)
Tel. +(34) 935 27 22 90 | www.namirial.com

Category	**PKI / QTSP**	Document ID	**PSC_PKI-3.1**	**UANATACA, S.A.**
Edited by	**Alejandro Grande**	Classification	**Public**	Legal Representative
Verified by	**AGR**	Version	**4.1**	**GGM**
Approved by	**GGM**	Date	**23/10/2026**	_____

Table of contents

Presentation 1

Introduction 1

Objective 1

Scope 1

Roles and responsibilities 1

Version control 2

1. DISCLOSURE TEXT APPLICABLE TO ELECTRONIC SIGNATURE AND AUTHENTICATION CERTIFICATES 2

1.1. Contact information 3

1.1.1. Responsible organization 3

1.1.2. Contact 3

1.1.3. Trusted Electronic Service Provider issuer 3

1.1.4. Contact for revocation processes 3

1.2. Types of Certificates 4

1.3. Purpose of the certificates 7

1.3.1. Common stipulations 7

1.4. Certificate usage limits 36

1.4.1. Usage limits directed at signatories 36

1.4.2. Usage limits directed at verifiers 36

1.5. Subscriber Obligations 38

1.5.1. Key generation 38

1.5.2. Application for certificates 38

1.5.3. Reporting obligations 38

1.6. Obligations of the signatories 39

1.6.1. Custodial obligations 39

1.6.2. Obligations of proper use 39

1.7. Obligations of the verifier 40

1.7.1. Informed decision 40

1.7.2. Electronic signature verification requirements 40

1.7.3. Trust in an unverified certificate 41

1.7.4. Effect of verification 41

1.7.5. Proper use and prohibited activities 41
1.7.6. Indemnity clause 41
1.8. UANATACA's Obligations 42
1.8.1. Regarding the provision of the digital certification service 42
1.8.2. Regarding the registration checks 43
1.8.3. Preservation periods 43
1.9. Limited warranties and warranty disclaimers 44
1.9.1. UANATACA's guarantee for digital certification services 44
1.9.2. Warranty Exclusion 45
1.10. Applicable Agreements and DPC 45
1.10.1. Applicable agreements 45
1.10.2. Certification Practice Statement 45
1.11. Rules of trust for long-established firms 45
1.12. Privacy policy 46
1.13. Privacy Policy 46
1.14. Refund policy 47
1.15. Applicable regulations and competent jurisdiction 47
1.16. Linkage with the list of Qualified Providers of Trusted Electronic Services 47
1.17. Divisibility of clauses, survival, full agreement and notification 47

Presentation

Introduction

In line with its broader strategic objectives, Uanataca SAU (UANATACA) has implemented across several areas the continuous evolution and update of the technical and organizational capabilities that support its Trust Services.

The ICT systems adopted must ensure both the maintenance of adequate levels of efficiency and effectiveness in operational management and the protection of information assets.

In the context of Information Security and Trust Services Management, it is therefore essential to guarantee compliance with current European and national regulatory frameworks.

Objective

The purpose of this document is to establish the regulatory, technical and operational framework applicable to the Trust Services provided by the organization.

Any exception to the provisions included in this document must be documented, traced and approved by the responsible governance body.

Scope

This policy applies to all areas, subscribers, relying parties and participants of UANATACA.

These provisions apply to the information systems, trust services and operational activities within the scope of the Qualified Trust Service Provider (QTSP).

This document is monitored and reviewed at least once a year or whenever significant organizational, technical or regulatory changes occur.

Roles and responsibilities

This document defines the requirements and obligations applicable to the participants, operators, subscribers and relying parties interacting with the Trust Services.

Version control

Version	Parts that change	Change description	Author	Date
1.0	Original	Document creation	AC	22/03/2016
1.1	Complete	New version of the document adding all signature profiles	DMP	12/05/2017
1.2	2	New certificate profiles are added to QSCD Centralized	ABD	05/09/2021
2	Complete	Review of the document regarding the new version of the Certification Practice Statement. Adjustment in accordance with the document coding of the Information Security Management System.	AGB	11/11/2021
3	1.1.1, 1.3.1	Update of registered office address of UANATACA SA Clarifying inclusion of attributes in certificates for the identification of interested parties before Public Administrations.	APV	06/06/2023
4	Complete	Adaptation of the document to the new corporate formats. Modification of the certificate profiles to which this PDS applies.	AGB	30/03/2026
4.1	Complete change	Adaptation to Namirial corporate formats due to change of company name	Alejandro Grande	23/10/2026

1. DISCLOSURE TEXT APPLICABLE TO ELECTRONIC SIGNATURE AND AUTHENTICATION CERTIFICATES

This document contains the essential information to know regarding the certification service of the Trusted Electronic Service Provider UANATACA.

1.1. Contact information

1.1.1. Responsible organization

The Trusted Electronic Service Provider Uanataca, SA, hereinafter "UANATACA", is an initiative of:

UANATACA, SA
MERIDIANA AVENUE, 350, 3RD FLOOR, 08027 BARCELONA
TELEPHONE: 935 272 290
EMAIL: INFO@UANATACA.COM

1.1.2. Contact

For any inquiries, please contact:

UANATACA, SA
EMAIL: INFO@UANATACA.COM
TELEPHONE: 935 272 290

1.1.3. Trusted Electronic Service Provider issuer

The certificates described in this document are issued by UANATACA, identified by the data indicated above.

1.1.4. Contact for revocation processes

For any inquiries, please contact:

UANATACA, SA
EMAIL: INFO@UANATACA.COM
TELEPHONE: 935 272 290

1.2. Types of Certificates

The following certificates issued by UANATACA are qualified in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the technical standard identified by reference ETSI EN 319 411-2. UANATACA has assigned each type of certificate an object identifier (OID) for identification by the applications, which are detailed below:

OID Number	Type of certificates	OID ETSI Policy	OID Uanataca
Qualified Certificate of Natural Person Citizen in software	QCP-n	0.4.0.194112.1.0	1.3.6.1.4.1.47286.1.1.1.1
Qualified Certificate of Natural Person Citizen in Centralized HSM	QCP-n	0.4.0.194112.1.0	1.3.6.1.4.1.47286.1.1.1.2
Qualified Certificate of Natural Person Citizen in QSCD	QCP-n-qscd	0.4.0.194112.1.2	1.3.6.1.4.1.47286.1.1.1.3
Qualified Certificate of Natural Person Citizen in centralized QSCD	QCP-n-qscd	0.4.0.194112.1.2	1.3.6.1.4.1.47286.1.1.1.4
Qualified Certificate of Signature of Natural Person Citizen in QSCD	QCP-n-qscd	0.4.0.194112.1.2	1.3.6.1.4.1.47286.1.1.1.5.1
Qualified Signature Certificate of a Natural Person Citizen in Centralized QSCD	QCP-n-qscd	0.4.0.194112.1.2	1.3.6.1.4.1.47286.1.1.1.5.2
Qualified Certificate of Natural Person Belonging to Software	QCP-n	0.4.0.194112.1.0	1.3.6.1.4.1.47286.1.1.2.1
Qualified Certificate of Natural Person Belonging to Centralized HSM	QCP-n	0.4.0.194112.1.0	1.3.6.1.4.1.47286.1.1.2.2
Qualified Certificate of Natural Person Belonging to QSCD	QCP-n-qscd	0.4.0.194112.1.2	1.3.6.1.4.1.47286.1.1.2.3
Qualified Certificate of Natural Person Belonging to Centralized QSCD	QCP-n-qscd	0.4.0.194112.1.2	1.3.6.1.4.1.47286.1.1.2.4

OID Number	Type of certificates	OID ETSI Policy	OID Uanataca
Qualified Signature Certificate of a Natural Person Belonging to QSCD	QCP-n-qscd	0.4.0.194112.1.2	1.3.6.1.4.1.47286.1.1.2.5.1
Qualified Signature Certificate of a Natural Person Belonging to a Centralized QSCD	QCP-n-qscd	0.4.0.194112.1.2	1.3.6.1.4.1.47286.1.1.2.5.2
Qualified Certificate of a Registered Individual in Software	QCP-n	0.4.0.194112.1.0	1.3.6.1.4.1.47286.1.1.3.1
Qualified Certificate of a Registered Individual in HSM Centralized	QCP-n	0.4.0.194112.1.0	1.3.6.1.4.1.47286.1.1.3.2
Qualified Certificate of Registered Individual in QSCD	QCP-n-qscd	0.4.0.194112.1.2	1.3.6.1.4.1.47286.1.1.3.3
Qualified Certificate of Registered Individual in QSCD Centralized	QCP-n-qscd	0.4.0.194112.1.2	1.3.6.1.4.1.47286.1.1.3.4
Qualified signature certificate of a registered individual in QSCD	QCP-n-qscd	0.4.0.194112.1.2	1.3.6.1.4.1.47286.1.1.3.5.1
Qualified signature certificate of a registered individual in centralized QSCD	QCP-n-qscd	0.4.0.194112.1.2	1.3.6.1.4.1.47286.1.1.3.5.2
of Natural Person Representative in software	QCP-n	0.4.0.194112.1.0	1.3.6.1.4.1.47286.1.2.1.1
Natural Person Representative in Centralized HSM	QCP-n	0.4.0.194112.1.0	1.3.6.1.4.1.47286.1.2.1.2
of Natural Person Representative in QSCD	QCP-n-qscd	0.4.0.194112.1.2	1.3.6.1.4.1.47286.1.2.1.3
Natural Person Representative in centralized QSCD	QCP-n-qscd	0.4.0.194112.1.2	1.3.6.1.4.1.47286.1.2.1.4
of Natural Person of signature Representative in software	QCP-n-qscd	0.4.0.194112.1.2	1.3.6.1.4.1.47286.1.2.2.1
of Natural Person of Representative signature in QSCD	QCP-n-qscd	0.4.0.194112.1.2	1.3.6.1.4.1.47286.1.2.2.2

OID Number	Type of certificates	OID ETSI Policy	OID Uanataca
of Natural Person of Representative signature in centralized QSCD	QCP-n-qscd	0.4.0.194112.1.2	1.3.6.1.4.1.47286.1.2.6.2
of Mid-Level Public Employee	QCP-n	0.4.0.194112.1.0	1.3.6.1.4.1.47286.1.4.1
High-Level Public Employee authentication	NCP+	0.4.0.2042.1.2	1.3.6.1.4.1.47286.1.4.2.1
Signature of a High-Level Public Employee	QCP-n-qscd	0.4.0.194112.1.2	1.3.6.1.4.1.47286.1.4.2.2
signature of a High-Level Public Employee in a centralized QSCD	QCP-n-qscd	0.4.0.194112.1.2	1.3.6.1.4.1.47286.1.4.6.2
Representative of a legal entity before the administrations in software	QCP-n	0.4.0.194112.1.0	1.3.6.1.4.1.47286.1.7.1
of a natural person Representative of a Legal Entity before the administrations in QSCD	QCP-n-qscd	0.4.0.194112.1.2	1.3.6.1.4.1.47286.1.7.2.2
Representative of a legal entity before the administrations in a centralized HSM (Hydrographic Management System)	QCP-n	0.4.0.194112.1.0	1.3.6.1.4.1.47286.1.7.5
Representative of a legal entity before the administrations in a centralized QSCD	QCP-n-qscd	0.4.0.194112.1.2	1.3.6.1.4.1.47286.1.7.6
of a natural person, Representative of an Entity without Legal Personality before the administrations in software	QCP-n	0.4.0.194112.1.0	1.3.6.1.4.1.47286.1.8.1
of a natural person, Representative of an Entity without Legal Personality before the administrations in QSCD	QCP-n-qscd	0.4.0.194112.1.2	1.3.6.1.4.1.47286.1.8.2.2
of a natural person, Representative of an Entity	QCP-n	0.4.0.194112.1.0	1.3.6.1.4.1.47286.1.8.5

OID Number	Type of certificates	OID ETSI Policy	OID Uanataca
without Legal Personality before the administrations in a centralized HSM			
of a natural person, Representative of an Entity without Legal Personality before the administrations in centralized QSCD	QCP-n-qscd	0.4.0.194112.1.2	1.3.6.1.4.1.47286.1.8.6

1.3. Purpose of the certificates

1.3.1. Common stipulations

The qualified certificates described in this document and issued in software and Centralized HSM, guarantee the identity of the subscriber and the person indicated in the certificate, allowing the generation of the “advanced electronic signature based on a qualified electronic certificate”.

The qualified certificates described in this document and issued in QSCD and QSCD Centralized operate with qualified signature creation devices, in accordance with Articles 29 and 51 of Regulation (EU) 910/2014, and comply with the technical standard of the European Telecommunications Standards Institute, identified by the reference EN 319 411-2 . These qualified certificates guarantee the identity of the signatory, allowing the generation of a “ qualified electronic signature”; that is, an advanced electronic signature based on a qualified certificate and generated using a qualified device, which is therefore equivalent to a handwritten signature for legal purposes, without the need to meet any other additional requirements.

Notwithstanding the foregoing, any type of qualified electronic certificate, when issued for the identification of interested parties before Public Administrations, must contain as attributes **its name** and **surname** and your **number National Identity Document, Foreigner Identification Number or Tax Identification Number** in an unambiguous manner as appropriate.

1.1.1 Qualified Certificate of Natural Person Citizen in software

This certificate has the OID 1.3.6.1.4.1.47286.1.1.1.1. It is a qualified certificate in accordance with Article 28 of Regulation (EU) 910/2014 eIDAS , issued for electronic signature and authentication, in accordance with the QCP-n certification policy with the OID 0.4.0.194112.1.0.

Certificates for individuals issued in software do not guarantee their operation with qualified signature creation devices, as referred to in Articles 29 and 51 of Regulation (EU) 910/2014.

These certificates guarantee the identity of the subscriber and the person indicated in the certificate, and allow the generation of the “advanced electronic signature based on a qualified electronic certificate”.

Certificates can be used in applications such as those listed below:

a) Authentication in access control systems.
b) Secure email signature.
c) Other electronic signature applications, in accordance with what the parties agree or with the legal rules applicable in each case.

The usage information in the certificate profile indicates the following:

The “key usage” field has the following functions enabled and therefore allows us to perform them:

a. signature (to perform the authentication function)
b. Content commitment (to perform the electronic signature function)
c. Key Encipherment

1.1.2 Qualified Certificate of Natural Person Citizen in Centralized HSM

This certificate has the OID 1.3.6.1.4.1.47286.1.1.1.2. It is a qualified certificate issued for advanced electronic signature and authentication, in accordance with the QCP-n certification policy with the OID 0.4.0.194112.1.0. Natural person certificates issued in

Centralized HSM are qualified certificates in accordance with the provisions of Articles 24 and 28 of Regulation (EU) 910/2014 .

They guarantee the identity of the subscriber and the person indicated in the certificate, and allow the generation of the “advanced electronic signature based on a qualified electronic certificate”.

Certificates can be used in applications such as those listed below:

a) Authentication in access control systems.
b) Secure email signature.
c) Other electronic signature applications, in accordance with what the parties agree or with the legal rules applicable in each case.

The usage information in the certificate profile indicates the following:

The “key usage” field has the following functions enabled and therefore allows us to perform them:

a. signature (to perform the authentication function)
b. Content commitment (to perform the electronic signature function)
c. Key Encipherment

1.1.3 Qualified Certificate of Natural Person Citizen in QSCD

This certificate has the OID 1.3.6.1.4.1.47286.1.1.1.3. It is a qualified certificate issued for qualified electronic signature and authentication, in accordance with the QCP-n-qscd certification policy with the OID 0.4.0.194112.1.2. This certificate issued in QSCD is a qualified certificate in accordance with Article 28 of Regulation (EU) 910/2014 eIDAS.

It works with qualified signature creation devices, in accordance with Articles 29 and 51 of Regulation (EU) 910/2014, and complies with the technical regulations of the European Telecommunications Standards Institute, identified by the reference EN 319 411-2 .

It guarantees the identity of the signatory and their connection to the subscriber of the trusted electronic service, and allows the generation of the "qualified electronic signature"; that is, the advanced electronic signature that is based on a qualified certificate and that has been generated using a qualified device, which is therefore equivalent to a written signature for legal effect, without the need to meet any other additional requirement.

It can also be used in applications that do not require an electronic signature equivalent to a handwritten signature, such as the applications listed below:

a) Secure email signature.
b) Other electronic signature applications.

The usage information in the certificate profile indicates the following:

The “key usage” field has the following functions enabled and therefore allows us to perform them:

a. signature (to perform the authentication function)
b. Content commitment (to perform the electronic signature function)
c. Key Encipherment

1.1.4 Qualified Certificate of Natural Person Citizen in centralized QSCD

This certificate has the OID 1.3.6.1.4.1.47286.1.1.1.4 . It is a qualified certificate issued for qualified electronic signature and authentication, in accordance with the QCP-n-qscd certification policy with the OID 0.4.0.194112.1.2. This certificate issued in centralized QSCD, is a qualified certificate in accordance with the provisions of Article 28 of Regulation (EU) 910/2014 eIDAS.

It works with qualified signature creation devices, in accordance with Articles 29 and 51 of Regulation (EU) 910/2014, and complies with the technical regulations of the European Telecommunications Standards Institute, identified by the reference EN 319 411-2 .

It guarantees the identity of the signatory and their connection to the subscriber of the trusted electronic service, and allows the generation of the "qualified electronic signature"; that is, the advanced electronic signature that is based on a qualified certificate and that has been generated using a qualified device, which is therefore equivalent to a written signature for legal effect, without the need to meet any other additional requirement.

It can also be used in applications that do not require an electronic signature equivalent to a written signature, such as the applications listed below:

a) Secure email signature.
b) Other electronic signature applications.

The usage information in the certificate profile indicates the following:

The “key usage” field has the following functions enabled and therefore allows us to perform them:

a. signature (to perform the authentication function)
b. Content commitment (to perform the electronic signature function)
c. Key Encipherment

1.1.5 Qualified Certificate of Signature of Natural Person Citizen in QSCD

This certificate has the OID 1.3.6.1.4.1.47286.1.1.2.5.1 . It is a qualified certificate issued for qualified electronic signatures , in accordance with the QCP-n-qscd certification policy with OID 0.4.0.194112.1.2, as stated in the certificate. This certificate , issued in QSCD, is a qualified certificate as established in Article 28 of Regulation (EU) 910/2014 eIDAS.

It works with qualified signature creation devices (QSCDs), in accordance with Articles 29 and 51 of Regulation (EU) 910/2014, and complies with the technical regulations of the European Telecommunications Standards Institute, identified by the reference EN 319 411-2 .

It guarantees the identity of the signatory and their connection to the subscriber of the trusted electronic service, and allows the generation of the "qualified electronic signature", that is, the advanced electronic signature that is based on a qualified certificate and that has been generated using a qualified device, which is therefore equivalent to a written signature for legal effect, without the need to meet any other additional requirement.

It can also be used in applications that do not require an electronic signature equivalent to a handwritten signature, such as the applications listed below:

a) Secure email signature.
b) Other electronic signature applications.

The usage information in the certificate profile indicates the following:

The “key usage” field has the following functions enabled, allowing us to perform them:

a. Content commitment (to perform the electronic signature function)

1.1.6 Qualified Signature Certificate of a Natural Person Citizen in Centralized QSCD

This certificate has the OID 1.3.6.1.4.1.47286.1.1.1.5.2 . It is a qualified certificate issued for qualified electronic signatures , in accordance with the QCP-n-qscd certification policy with OID 0.4.0.194112.1.2, as stated in the certificate. This certificate, issued in a centralized QSCD, is a qualified certificate as established in Article 28 of Regulation (EU) 910/2014 eIDAS.

It works with qualified signature creation devices (QSCDs), in accordance with Articles 29 and 51 of Regulation (EU) 910/2014, and complies with the technical regulations of the European Telecommunications Standards Institute, identified by the reference EN 319 411-2 .

It guarantees the identity of the signatory and their connection to the subscriber of the trusted electronic service, and allows the generation of the "qualified electronic signature", that is, the advanced electronic signature that is based on a qualified certificate and that has been generated using a qualified device, which is therefore equivalent to a written signature for legal effect, without the need to meet any other additional requirement.

It can also be used in applications that do not require an electronic signature equivalent to a handwritten signature, such as the applications listed below:

a) Secure email signature.
b) Other electronic signature applications.

The usage information in the certificate profile indicates the following:

The “key usage” field has the following functions enabled, allowing us to perform them:

a. Content commitment (to perform the electronic signature function)

1.1.7 Qualified Certificate of Natural Person Belonging to Software

This certificate has the OID 1.3.6.1.4.1.47286.1.1.2.1. It is a qualified certificate in accordance with Article 28 of Regulation (EU) 910/2014 eIDAS , issued for electronic signature and authentication, in accordance with the QCP-n certification policy with the OID 0.4.0.194112.1.0.

Certificates for individuals issued in software do not guarantee their operation with qualified signature creation devices, as referred to in Articles 29 and 51 of Regulation (EU) 910/2014.

These certificates guarantee the identity of the subscriber and the person indicated in the certificate, and allow the generation of the “advanced electronic signature based on a qualified electronic certificate”.

Certificates can be used in applications such as those listed below:

d) Authentication in access control systems.
e) Secure email signature.
f) Other electronic signature applications, in accordance with what the parties agree or with the legal rules applicable in each case.

The usage information in the certificate profile indicates the following:

The “key usage” field has the following functions enabled and therefore allows us to perform them:

d. signature (to perform the authentication function)
e. Content commitment (to perform the electronic signature function)
f. Key Encipherment

1.1.8 Qualified Certificate of Natural Person Belonging to Centralized HSM

This certificate has the OID 1.3.6.1.4.1.47286.1.1.2.2. It is a qualified certificate issued for advanced electronic signature and authentication, in accordance with the QCP-n certification policy with the OID 0.4.0.194112.1.0. Natural person certificates issued in Centralized HSM are qualified certificates in accordance with the provisions of Articles 24 and 28 of Regulation (EU) 910/2014 .

They guarantee the identity of the subscriber and the person indicated in the certificate, and allow the generation of the "advanced electronic signature based on a qualified electronic certificate".

Certificates can be used in applications such as those listed below:

d) Authentication in access control systems.
e) Secure email signature.
f) Other electronic signature applications, in accordance with what the parties agree or with the legal rules applicable in each case.

The usage information in the certificate profile indicates the following:

The “key usage” field has the following functions enabled and therefore allows us to perform them:

d. signature (to perform the authentication function)
e. Content commitment (to perform the electronic signature function)
f. Key Encipherment

1.1.9 Qualified Certificate of Natural Person Belonging to QSCD

This certificate has the OID 1.3.6.1.4.1.47286.1.1.2.3 . It is a qualified certificate issued for qualified electronic signature and authentication, in accordance with the QCP-n-qscd certification policy with the OID 0.4.0.194112.1.2. This certificate issued in QSCD is a qualified certificate in accordance with Article 28 of Regulation (EU) 910/2014 eIDAS.

It works with qualified signature creation devices, in accordance with Articles 29 and 51 of Regulation (EU) 910/2014, and complies with the technical regulations of the European Telecommunications Standards Institute, identified by the reference EN 319 411-2 .

It guarantees the identity of the signatory and their connection to the subscriber of the trusted electronic service, and allows the generation of the "qualified electronic signature"; that is, the advanced electronic signature that is based on a qualified certificate and that has been generated using a qualified device, which is therefore equivalent to a written signature for legal effect, without the need to meet any other additional requirement.

It can also be used in applications that do not require an electronic signature equivalent to a handwritten signature, such as the applications listed below:

c) Secure email signature.
d) Other electronic signature applications.

The usage information in the certificate profile indicates the following:

The “key usage” field has the following functions enabled and therefore allows us to perform them:

d. signature (to perform the authentication function)
e. Content commitment (to perform the electronic signature function)
f. Key Encipherment

1.1.10 Qualified Certificate of Natural Person Belonging to Centralized QSCD

This certificate has the OID 1.3.6.1.4.1.47286.1.1.2.4 . It is a qualified certificate issued for qualified electronic signature and authentication, in accordance with the QCP-n-qscd certification policy with the OID 0.4.0.194112.1.2. This certificate issued in centralized QSCD is a qualified certificate in accordance with the provisions of Article 28 of Regulation (EU) 910/2014 eIDAS.

It works with qualified signature creation devices, in accordance with Articles 29 and 51 of Regulation (EU) 910/2014, and complies with the technical regulations of the European Telecommunications Standards Institute, identified by the reference EN 319 411-2 .

It guarantees the identity of the signatory and their connection to the subscriber of the trusted electronic service, and allows the generation of the "qualified electronic signature"; that is, the advanced electronic signature that is based on a qualified certificate and that has been generated using a qualified device, which is therefore

equivalent to a written signature for legal effect, without the need to meet any other additional requirement.

It can also be used in applications that do not require an electronic signature equivalent to a handwritten signature, such as the applications listed below:

c) Secure email signature.
d) Other electronic signature applications.

The usage information in the certificate profile indicates the following:

The “key usage” field has the following functions enabled and therefore allows us to perform them:

d. signature (to perform the authentication function)
e. Content commitment (to perform the electronic signature function)
f. Key Encipherment

1.1.11 Qualified Signature Certificate of a Natural Person Belonging to QSCD

This certificate has the OID 1.3.6.1.4.1.47286.1.1.2.5.1 . It is a qualified certificate issued for qualified electronic signatures , in accordance with the QCP-n-qscd certification policy with OID 0.4.0.194112.1.2, as stated in the certificate. This certificate , issued in QSCD, is a qualified certificate as established in Article 28 of Regulation (EU) 910/2014 eIDAS.

It works with qualified signature creation devices (QSCDs), in accordance with Articles 29 and 51 of Regulation (EU) 910/2014, and complies with the technical regulations of the European Telecommunications Standards Institute, identified by the reference EN 319 411-2 .

It guarantees the identity of the signatory and their connection to the subscriber of the trusted electronic service, and allows the generation of the "qualified electronic signature", that is, the advanced electronic signature that is based on a qualified certificate and that has been generated using a qualified device, which is therefore equivalent to a written signature for legal effect, without the need to meet any other additional requirement.

It can also be used in applications that do not require an electronic signature equivalent to a handwritten signature, such as the applications listed below:

c) Secure email signature.
d) Other electronic signature applications.

The usage information in the certificate profile indicates the following:

The “key usage” field has the following functions enabled, allowing us to perform them:

b. Content commitment (to perform the electronic signature function)

1.1.12 Qualified Signature Certificate of a Natural Person Belonging to a Centralized QSCD

This certificate has the OID 1.3.6.1.4.1.47286.1.1.2.5.2 . It is a qualified certificate issued for qualified electronic signatures , in accordance with the QCP-n-qscd certification policy with OID 0.4.0.194112.1.2, as stated in the certificate. This certificate, issued in a centralized QSCD, is a qualified certificate as established in Article 28 of Regulation (EU) 910/2014 eIDAS.

It works with qualified signature creation devices (QSCDs), in accordance with Articles 29 and 51 of Regulation (EU) 910/2014, and complies with the technical regulations of the European Telecommunications Standards Institute, identified by the reference EN 319 411-2 .

It guarantees the identity of the signatory and their connection to the subscriber of the trusted electronic service, and allows the generation of the "qualified electronic signature", that is, the advanced electronic signature that is based on a qualified certificate and that has been generated using a qualified device, which is therefore equivalent to a written signature for legal effect, without the need to meet any other additional requirement.

It can also be used in applications that do not require an electronic signature equivalent to a handwritten signature, such as the applications listed below:

c) Secure email signature.
d) Other electronic signature applications.

The usage information in the certificate profile indicates the following:

The “key usage” field has the following functions enabled, allowing us to perform them:

b. Content commitment (to perform the electronic signature function)

1.1.13 Qualified Certificate of a Registered Individual in Software

This certificate has the OID 1.3.6.1.4.1.47286.1.1.3.1. It is a qualified certificate in accordance with Article 28 of Regulation (EU) 910/2014 eIDAS , issued for electronic signature and authentication, in accordance with the QCP-n certification policy with the OID 0.4.0.194112.1.0.

Certificates for individuals issued in software do not guarantee their operation with qualified signature creation devices, as referred to in Articles 29 and 51 of Regulation (EU) 910/2014.

These certificates guarantee the identity of the subscriber and the person indicated in the certificate, and allow the generation of the "advanced electronic signature based on a qualified electronic certificate".

Certificates can be used in applications such as those listed below:

g) Authentication in access control systems.
h) Secure email signature.
i) Other electronic signature applications, in accordance with what the parties agree or with the legal rules applicable in each case.

The usage information in the certificate profile indicates the following:

The "key usage" field has the following functions enabled and therefore allows us to perform them:

g. signature (to perform the authentication function)
h. Content commitment (to perform the electronic signature function)
i. Key Encipherment

1.1.14 Qualified Certificate of a Registered Individual in HSM Centralized

This certificate has the OID 1.3.6.1.4.1.47286.1.1.3.2. It is a qualified certificate issued for advanced electronic signature and authentication, in accordance with the QCP-n certification policy with the OID 0.4.0.194112.1.0. Natural person certificates issued in Centralized HSM are qualified certificates in accordance with the provisions of Articles 24 and 28 of Regulation (EU) 910/2014 .

They guarantee the identity of the subscriber and the person indicated in the certificate, and allow the generation of the "advanced electronic signature based on a qualified electronic certificate".

Certificates can be used in applications such as those listed below:

g) Authentication in access control systems.
h) Secure email signature.
i) Other electronic signature applications, in accordance with what the parties agree or with the legal rules applicable in each case.

The usage information in the certificate profile indicates the following:

The “key usage” field has the following functions enabled and therefore allows us to perform them:

g. signature (to perform the authentication function)
h. Content commitment (to perform the electronic signature function)
i. Key Encipherment

1.1.15 Qualified Certificate of Registered Individual in QSCD

This certificate has the OID 1.3.6.1.4.1.47286.1.1.3.3. It is a qualified certificate issued for qualified electronic signature and authentication, in accordance with the QCP-n-qscd certification policy with the OID 0.4.0.194112.1.2. This certificate issued in QSCD is a qualified certificate in accordance with Article 28 of Regulation (EU) 910/2014 eIDAS.

It works with qualified signature creation devices, in accordance with Articles 29 and 51 of Regulation (EU) 910/2014, and complies with the technical regulations of the European Telecommunications Standards Institute, identified by the reference EN 319 411-2 .

It guarantees the identity of the signatory and their connection to the subscriber of the trusted electronic service, and allows the generation of the "qualified electronic signature"; that is, the advanced electronic signature that is based on a qualified certificate and that has been generated using a qualified device, which is therefore equivalent to a written signature for legal effect, without the need to meet any other additional requirement.

It can also be used in applications that do not require an electronic signature equivalent to a written signature, such as the applications listed below:

e) Secure email signature.
f) Other electronic signature applications.

The usage information in the certificate profile indicates the following:

The “key usage” field has the following functions enabled and therefore allows us to perform them:

g. signature (to perform the authentication function)

h. Content commitment (to perform the electronic signature function)
i. Key Encipherment

1.1.16 Qualified Certificate of a Registered Individual in QSCD Centralized

This certificate has the OID 1.3.6.1.4.1.47286.1.1.3.4 . It is a qualified certificate issued for qualified electronic signature and authentication, in accordance with the QCP-n-qscd certification policy with the OID 0.4.0.194112.1.2. This certificate issued in centralized QSCD, is a qualified certificate in accordance with the provisions of Article 28 of Regulation (EU) 910/2014 eIDAS.

It works with qualified signature creation devices, in accordance with Articles 29 and 51 of Regulation (EU) 910/2014, and complies with the technical regulations of the European Telecommunications Standards Institute, identified by the reference EN 319 411-2 .

It guarantees the identity of the signatory and their connection to the subscriber of the trusted electronic service, and allows the generation of the "qualified electronic signature"; that is, the advanced electronic signature that is based on a qualified certificate and that has been generated using a qualified device, which is therefore equivalent to a written signature for legal effect, without the need to meet any other additional requirement.

It can also be used in applications that do not require an electronic signature equivalent to a handwritten signature, such as the applications listed below:

e) Secure email signature.
f) Other electronic signature applications.

The usage information in the certificate profile indicates the following:

The “key usage” field has the following functions enabled and therefore allows us to perform them:

g. signature (to perform the authentication function)
h. Content commitment (to perform the electronic signature function)
i. Key Encipherment

1.1.17 Qualified signature certificate of a registered individual in QSCD

This certificate has the OID 1.3.6.1.4.1.47286.1.1.3.5.1 . It is a qualified certificate issued for qualified electronic signatures , in accordance with the QCP-n-qscd certification policy with OID 0.4.0.194112.1.2, as stated in the certificate. This certificate , issued in QSCD, is a qualified certificate as established in Article 28 of Regulation (EU) 910/2014 eIDAS.

It works with qualified signature creation devices (QSCDs), in accordance with Articles 29 and 51 of Regulation (EU) 910/2014, and complies with the technical regulations of the European Telecommunications Standards Institute, identified by the reference EN 319 411-2 .

It guarantees the identity of the signatory and their connection to the subscriber of the trusted electronic service, and allows the generation of the "qualified electronic signature", that is, the advanced electronic signature that is based on a qualified certificate and that has been generated using a qualified device, which is therefore equivalent to a written signature for legal effect, without the need to meet any other additional requirement.

It can also be used in applications that do not require an electronic signature equivalent to a handwritten signature, such as the applications listed below:

e) Secure email signature.
f) Other electronic signature applications.

The usage information in the certificate profile indicates the following:

The “key usage” field has the following functions enabled, allowing us to perform them:

c. Content commitment (to perform the electronic signature function)

1.1.18 Qualified signature certificate of a registered individual in centralized QSCD

This certificate has the OID 1.3.6.1.4.1.47286.1.1.3.5.2 . It is a qualified certificate issued for qualified electronic signatures , in accordance with the QCP-n-qscd certification policy with OID 0.4.0.194112.1.2, as stated in the certificate. This certificate, issued in a centralized QSCD, is a qualified certificate as established in Article 28 of Regulation (EU) 910/2014 eIDAS.

It works with qualified signature creation devices (QSCDs), in accordance with Articles 29 and 51 of Regulation (EU) 910/2014, and complies with the technical regulations of the European Telecommunications Standards Institute, identified by the reference EN 319 411-2 .

It guarantees the identity of the signatory and their connection to the subscriber of the trusted electronic service, and allows the generation of the "qualified electronic signature", that is, the advanced electronic signature that is based on a qualified certificate and that has been generated using a qualified device, which is therefore equivalent to a written signature for legal effect, without the need to meet any other additional requirement.

It can also be used in applications that do not require an electronic signature equivalent to a written signature, such as the applications listed below:

e) Secure email signature.
f) Other electronic signature applications.

The usage information in the certificate profile indicates the following:

The “key usage” field has the following functions enabled, allowing us to perform them:

c. Content commitment (to perform the electronic signature function)

1.1.19 Qualified Certificate of Natural Person Representative in Software

This certificate has the OID 1.3.6.1.4.1.47286.1.2.1.1. It is a qualified certificate issued for advanced electronic signature and authentication, in accordance with the QCP-n certification policy with the OID 0.4.0.194112.1.0. se, of a natural person or representative of an entity issued in software in accordance with the provisions of Article 28 of Regulation (EU) 910/2014 eIDAS, and which complies with the provisions of the technical regulations of the European Institute of Telecommunications Standards, identified with the reference EN 319 411-2 .

They guarantee the identity of the subscriber and the signatory, and a legal representation or power of attorney relationship between the signatory and an entity, company or organization described in the “O” (Organization) field, and allow the generation of the “advanced electronic signature based on a qualified electronic certificate” .

Furthermore, representative certificates issued in software can be used in other applications such as those listed below:

a) Authentication in access control systems.
b) Secure email signature.
c) Other electronic signature applications.

The usage information in the certificate profile indicates the following:

The “key usage” field has the following functions enabled and therefore allows us to perform them:

a. signature (to perform the authentication function)
b. Content commitment (to perform the electronic signature function)
c. Key Encipherment

1.1.20 Qualified Certificate of Natural Person Representative in Centralized HSM

This certificate has the OID 1.3.6.1.4.1.47286.1.2.1.2. It is a qualified certificate issued for advanced electronic signature and authentication, in accordance with the QCP-n certification policy with the OID 0.4.0.194112.1.0. , of a natural person or representative of an entity issued in a Centralized HSM in accordance with the provisions of Article 28 of Regulation (EU) 910/2014 eIDAS, and which complies with the provisions of the technical regulations of the European Institute of Telecommunications Standards, identified with the reference EN 319 411-2 .

They guarantee the identity of the subscriber and the signatory, and a legal representation or power of attorney relationship between the signatory and an entity, company or organization described in the “O” (Organization) field, and allow the generation of the “advanced electronic signature based on a qualified electronic certificate” .

Furthermore, representative certificates issued in software can be used in other applications such as those listed below:

a) Authentication in access control systems.
b) Secure email signature.
c) Other electronic signature applications.

The usage information in the certificate profile indicates the following:

The “key usage” field has the following functions enabled and therefore allows us to perform them:

a. signature (to perform the authentication function)
b. Content commitment (to perform the electronic signature function)
c. Key Encipherment

1.1.21 Qualified Certificate of Natural Person Representative in QSCD

This certificate has the OID 1.3.6.1.4.1.47286.1.2.1.2. It is a qualified certificate issued for advanced electronic signature and authentication, in accordance with the QCP-n certification policy with the OID 0.4.0.194112.1.0. , of a natural person or representative of an entity issued in QSCD in accordance with the provisions of Article 28 of Regulation (EU) 910/2014 eIDAS, and which complies with the provisions of the technical regulations of the European Institute of Telecommunications Standards, identified with the reference EN 319 411-2 .

They guarantee the identity of the subscriber and the signatory, and a legal representation or power of attorney relationship between the signatory and an entity, company or organization described in the "O" (Organization) field, and allow the generation of the "qualified electronic signature based on a qualified electronic certificate" .

Furthermore, representative certificates issued in software can be used in other applications such as those listed below:

a) Authentication in access control systems.
b) Secure email signature.
c) Other electronic signature applications.

The usage information in the certificate profile indicates the following:

The "key usage" field has the following functions enabled and therefore allows us to perform them:

a. signature (to perform the authentication function)
b. Content commitment (to perform the electronic signature function)
c. Key Encipherment

1.1.22 Qualified Certificate of Natural Person Representative in Centralized QSCD

This certificate has the OID 1.3.6.1.4.1.47286.1.2.1.2. It is a qualified certificate issued for advanced electronic signature and authentication, in accordance with the QCP-n certification policy with the OID 0.4.0.194112.1.0. , of a natural person or representative of an entity issued in QSCD in accordance with the provisions of Article 28 of Regulation (EU) 910/2014 eIDAS, and which complies with the provisions of the technical regulations of the European Institute of Telecommunications Standards, identified with the reference EN 319 411-2 .

They guarantee the identity of the subscriber and the signatory, and a legal representation or power of attorney relationship between the signatory and an entity, company or organization described in the "O" (Organization) field, and allow the generation of the "qualified electronic signature based on a qualified electronic certificate" .

Furthermore, representative certificates issued in software can be used in other applications such as those listed below:

d) Authentication in access control systems.
e) Secure email signature.
f) Other electronic signature applications.

The usage information in the certificate profile indicates the following:

The "key usage" field has the following functions enabled and therefore allows us to perform them:

d. signature (to perform the authentication function)
e. Content commitment (to perform the electronic signature function)
f. Key Encipherment

1.1.23 Certified Qualified Individual Signature Representative in Software

This certificate has the OID 1.3.6.1.4.1.47286.1.2.2.1. It is a qualified certificate issued for qualified electronic signatures, in accordance with the QCP-n-qscd certification policy with the OID 0.4.0.194112.1.2. This representative certificate issued in QSCD is a qualified certificate in accordance with Article 28 of Regulation (EU) 910/2014 eIDAS.

It works with qualified signature creation devices, in accordance with Articles 29 and 51 of Regulation (EU) 910/2014 , and complies with the technical regulations of the European Telecommunications Standards Institute, identified by the reference EN 319 411-2 .

It guarantees the identity of the subscriber and the signatory, and a legal representation or power of attorney relationship between the signatory and an entity, company or organization described in the "O" (Organization) field, and allows the generation of the "qualified electronic signature" that is, the advanced electronic signature that is based on a qualified certificate and that has been generated using a qualified device, which is equivalent to a written signature for legal effect, without the need to meet any other additional requirement.

It can also be used in applications that do not require an electronic signature equivalent to a handwritten signature, such as the applications listed below:

a) Secure email signature.
b) Other electronic signature applications.

The usage information in the certificate profile indicates the following:

The “key usage” field has the following functions enabled and therefore allows us to perform them:

a. Content commitment (to perform the electronic signature function)

1.1.24 Certified Qualified Individual Signature Representative at QSCD

This certificate has the OID 1.3.6.1.4.1.47286.1.2.2.2. It is a qualified certificate issued for qualified electronic signatures, in accordance with the QCP-n-qscd certification policy with the OID 0.4.0.194112.1.2. This representative certificate issued in QSCD is a qualified certificate in accordance with Article 28 of Regulation (EU) 910/2014 eIDAS.

It works with qualified signature creation devices, in accordance with Articles 29 and 51 of Regulation (EU) 910/2014 , and complies with the technical regulations of the European Telecommunications Standards Institute, identified by the reference EN 319 411-2 .

It guarantees the identity of the subscriber and the signatory, and a legal representation or power of attorney relationship between the signatory and an entity, company or organization described in the “O” (Organization) field, and allows the generation of the “qualified electronic signature” that is, the advanced electronic signature that is based on a qualified certificate and that has been generated using a qualified device, which is therefore equivalent to a written signature for legal effect, without the need to meet any other additional requirement.

It can also be used in applications that do not require an electronic signature equivalent to a written signature, such as the applications listed below:

c) Secure email signature.
d) Other electronic signature applications.

The usage information in the certificate profile indicates the following:

The “key usage” field has the following functions enabled and therefore allows us to perform them:

b. Content commitment (to perform the electronic signature function)

1.1.25 Qualified Certificate of Natural Person Signature Representative in Centralized QSCD

This certificate has the OID 1.3.6.1.4.1.4 7286. 1 . 2.6.2. It is a qualified certificate issued for qualified electronic signatures, in accordance with the QCP-n-qscd certification policy with the OID 0.4.0.194112.1.2. This representative certificate issued in centralized QSCD is a qualified certificate in accordance with the provisions of Article 28 of Regulation (EU) 910/2014 eIDAS.

It works with qualified signature creation devices, in accordance with Articles 29 and 51 of Regulation (EU) 910/2014 , and complies with the technical regulations of the European Telecommunications Standards Institute, identified by the reference EN 319 411-2 .

It guarantees the identity of the subscriber and the signatory, and a legal representation or power of attorney relationship between the signatory and an entity, company or organization described in the "O" (Organization) field, and allows the generation of the "qualified electronic signature" that is, the advanced electronic signature that is based on a qualified certificate and that has been generated using a qualified device, which is equivalent to a written signature for legal effect, without the need to meet any other additional requirement.

It can also be used in applications that do not require an electronic signature equivalent to a handwritten signature, such as the applications listed below:

a) Secure email signature.
b) Other electronic signature applications.

The usage information in the certificate profile indicates the following:

The "key usage" field has the following functions enabled and therefore allows us to perform them:

a. Content commitment (to perform the electronic signature function)

1.1.26 Qualified Certificate of Mid-Level Public Employee

This certificate has the OID 1.3.6.1.4.1.4728 6.1 .4.1. It is a qualified certificate issued for advanced electronic signature and authentication, in accordance with the QCP-n certification policy with OID 0.4.0.194112.1.0. Mid-level public employee certificates are qualified certificates in accordance with Article 28 of Regulation (EU) 910/2014 eIDAS.

These certificates are issued to public employees to identify them as individuals serving the Public Administration, linking them to it, in compliance with the requirements

established in Article 43 of Law 40/2015, of October 1, on the Legal Regime of the Public Sector. They are issued in accordance with the Electronic Identification and Signature Scheme of Public Administrations in its version in force at the date of this document.

It guarantees the identity of the subscriber and the person indicated in the certificate, and allows the generation of the "advanced electronic signature based on a qualified electronic certificate".

They can also be used in applications that do not require an electronic signature equivalent to a written signature, such as the applications listed below:

a) Secure email signature.
b) Other electronic signature applications.

The usage information in the certificate profile indicates the following:

The “key usage” field has the following functions enabled, and therefore allows us to perform them:

a. signature (to perform the authentication function)
b. Content commitment (to perform the electronic signature function)
c. Key Encipherment

1.1.27 Electronic Authentication Certificate for High-Level Public Employees

This certificate has the OID 1.3.6.1.4.1.47286.1.4.2.1. It is a certificate issued for authentication purposes, in accordance with the NCP+ certification policy. This certificate is issued to public employees to identify them as individuals serving the Public Administration, linking them to it.

This authentication certificate works with qualified signature creation devices, in accordance with Articles 29 and 51 of Regulation (EU) 910/2014 eIDAS , and is issued in accordance with the Electronic Identification and Signature Scheme of Public Administrations in its current version as of the date of this document.

The usage information in the certificate profile indicates the following:

The “key usage” field has the following functions enabled, and therefore allows them to be performed:

a. signature (to perform the authentication function)
b. Key Encipherment

1.1.28 Qualified Signature Certificate of a High-Level Public Employee

This certificate has the OID 1.3.6.1.4.1.47286 .1.4. 2.2. It is a qualified certificate issued for qualified electronic signatures, in accordance with the QCP-n-qscd certification policy with the OID 0.4.0.194112.1.2. This certificate is qualified in accordance with the provisions of Article 28 of Regulation (EU) 910/2014 eIDAS.

This qualified certificate is issued to public employees to identify them as persons in the service of the Public Administration, linking them with it, fulfilling the requirements established in article 43 of Law 40/2015, of October 1, on the Legal Regime of the Public Sector, for the electronic signature of the personnel in the service of the Public Administrations.

It works with qualified signature creation devices, in accordance with Articles 29 and 51 of Regulation (EU) 910/2014, and complies with the technical regulations of the European Telecommunications Standards Institute, identified by the reference EN 319 411-2 . It is issued in accordance with the Electronic Identification and Signature Scheme of Public Administrations in its version in force at the date of this document.

It guarantees the identity of the subscriber and the signatory, and allows the generation of the “qualified electronic signature”; that is, the advanced electronic signature that is based on a qualified certificate and that has been generated using a qualified device, which, in accordance with the provisions of Article 25.2 of Regulation (EU) 910/2014, is equivalent to a written signature for legal effect, without the need to comply with any other additional requirement.

They can also be used in other applications such as those listed below:

a) Secure email signature.
b) Other electronic signature applications.

The usage information in the certificate profile indicates the following:

The “key usage” field has the following functions enabled, and therefore allows them to be performed:

a. Content commitment (to perform the electronic signature function)

1.1.29 Qualified Signature Certificate of a Senior Public Employee in Centralized QSCD

This certificate has the OID 1.3.6.1.4.1.47286 .1.4. 6.2. It is a qualified certificate issued for qualified electronic signature, in accordance with the QCP-n-qscd certification policy with

the OID 0.4.0.194112.1.2. This certificate is qualified in accordance with the provisions of Article 28 of Regulation (EU) 910/2014 eIDAS.

This qualified certificate is issued to public employees to identify them as persons in the service of the Public Administration, linking them with it, fulfilling the requirements established in article 43 of Law 40/2015, of October 1, on the Legal Regime of the Public Sector, for the electronic signature of the personnel in the service of the Public Administrations.

This certificate, issued in a centralized QSCD, works with qualified signature creation devices, in accordance with Articles 29 and 51 of Regulation (EU) 910/2014, and complies with the technical regulations of the European Telecommunications Standards Institute, identified by the reference EN 319 411-2 . It is issued in accordance with the Electronic Identification and Signature Scheme of Public Administrations in its version in force at the date of this document.

It guarantees the identity of the subscriber and the signatory, and allows the generation of the "qualified electronic signature"; that is, the advanced electronic signature that is based on a qualified certificate and that has been generated using a qualified device, which, in accordance with the provisions of Article 25.2 of Regulation (EU) 910/2014, is equivalent to a written signature for legal effect, without the need to comply with any other additional requirement.

They can also be used in other applications such as those listed below:

a) Secure email signature.
b) Other electronic signature applications.

The usage information in the certificate profile indicates the following:

The "key usage" field has the following functions enabled, and therefore allows them to be performed:

a. Content commitment (to perform the electronic signature function)

1.1.30 Qualified certificate of natural person Representative of Legal Entity before the administrations in software

This certificate has the OID 1.3.6.1.4.1.47286.1.7.1. It is a qualified certificate issued for advanced electronic signature and authentication, in accordance with the QCP-n certification policy with the OID 0.4.0.194112.1.0.

This software-issued certificate is a qualified certificate in accordance with Article 28 of Regulation (EU) 910/2014 eIDAS, and complies with the technical regulations of the European Telecommunications Standards Institute, identified by the reference EN 319 411-2.

It guarantees the identity of the subscriber and the signatory, and a legal representation or power of attorney relationship between the signatory and an entity, company or organization described in the “O” (Organization) field, and allows the generation of the “advanced electronic signature based on a qualified electronic certificate” .

Furthermore, representative certificates issued in software can be used in other applications such as those listed below:

a) Authentication in access control systems.
b) Secure email signature.
c) Other electronic signature applications.

The usage information in the certificate profile indicates the following:

The “key usage” field has the following functions enabled and therefore allows us to perform them:

a. signature (to perform the authentication function)
b. Content commitment (to perform the electronic signature function)
c. Key Encipherment

1.1.31 Qualified certificate of natural person Representative of a Legal Entity before the administrations in QSCD

This certificate has the OID 1.3.6.1.4.1.47286 . 1 .7. 2.2. It is a qualified certificate issued for qualified electronic signature and authentication, in accordance with the QCP-n-qscd certification policy with the OID 0.4.0.194112.1.2, which is declared in the certificate.

This certificate issued in QSCD is a qualified certificate in accordance with Article 28 of Regulation (EU) 910/2014 eIDAS , and works with qualified signature creation devices, in accordance with Articles 29 and 51 of Regulation (EU) 910/2014 , and complies with the technical regulations of the European Telecommunications Standards Institute, identified by the reference EN 319 411-2 .

It guarantees the identity of the subscriber and the signatory, and a legal representation or power of attorney relationship between the signatory and an entity, company or organization described in the "O" (Organization) field, and allows the generation of the "qualified electronic signature" that is, the advanced electronic signature that is based on a qualified certificate and that has been generated using a qualified device, which is equivalent to a written signature for legal effect, without the need to meet any other additional requirement.

They can also be used in applications that do not require an electronic signature equivalent to a written signature, such as the applications listed below:

a) Secure email signature.
b) Other electronic signature applications.

The usage information in the certificate profile indicates the following:

The "key usage" field has the following functions enabled and therefore allows us to perform them:

a. signature (to perform the authentication function)
b. Content commitment (to perform the electronic signature function)
c. Key Encipherment

1.1.32 Qualified certificate of natural person Representative of Legal Entity before the administrations in HSM Centralized

This certificate has the OID 1.3.6.1.4.1.4728 6.1 .7.5. It is a qualified certificate issued for advanced electronic signature and authentication, in accordance with the QCP-n certification policy with the OID 0.4.0.194112.1.0, which is stated in the certificate.

It is a qualified certificate in accordance with the provisions of Article 28 of Regulation (EU) 910/2014 eIDAS, and complies with the technical regulations of the European Telecommunications Standards Institute, identified by the reference EN 319 411-2.

It guarantees the identity of the subscriber and the signatory, and a legal representation or power of attorney relationship between the signatory and an entity, company or organization described in the "O" (Organization) field, and allows the generation of the "advanced electronic signature based on a qualified electronic certificate" .

Furthermore, certificates can be used in other applications such as those listed below:

a) Authentication in access control systems.
b) Secure email signature.

c) Other electronic signature applications.

The usage information in the certificate profile indicates the following:

The “key usage” field has the following functions enabled and therefore allows us to perform them:

a. signature (to perform the authentication function)
b. Content commitment (to perform the electronic signature function)
c. Key Encipherment

1.1.33 Qualified certificate of natural person Representative of Legal Entity before the administrations in centralized QSCD

This certificate has the OID 1.3.6.1.4.1.47286.1.7.6 . It is a qualified certificate issued for qualified electronic signature and authentication, in accordance with the QCP-n - qscd certification policy with the OID 0.4.0.194112.1.2, which is declared in the certificate.

This certificate issued in centralized QSCD is a qualified certificate in accordance with Article 28 of Regulation (EU) 910/2014 eIDAS , and works with qualified signature creation devices, in accordance with Articles 29 and 51 of Regulation (EU) 910/2014 , and complies with the technical regulations of the European Telecommunications Standards Institute, identified with the reference EN 319 411-2 .

It guarantees the identity of the subscriber and the signatory, and a legal representation or power of attorney relationship between the signatory and an entity, company or organization described in the “O” (Organization) field, and allows the generation of the “qualified electronic signature” that is, the advanced electronic signature that is based on a qualified certificate and that has been generated using a qualified device, which is equivalent to a written signature for legal effect, without the need to meet any other additional requirement.

They can also be used in applications that do not require an electronic signature equivalent to a written signature, such as the applications listed below:

a) Secure email signature.
b) Other electronic signature applications.

The usage information in the certificate profile indicates the following:

The “key usage” field has the following functions enabled and therefore allows us to perform them:

a. signature (to perform the authentication function)

b. Content commitment (to perform the electronic signature function)
c. Key Encipherment

1.1.34 Qualified certificate of natural person Representative of an Entity without Legal Personality before the administrations in software

This certificate has the OID 1.3.6.1.4.1.47286.1.8.1. It is a qualified certificate issued for advanced electronic signature and authentication, in accordance with the QCP-n certification policy with the OID 0.4.0.194112.1.0, which is stated in the certificate.

It is a qualified certificate in accordance with the provisions of Article 28 of Regulation (EU) 910/2014, and complies with the technical regulations of the European Institute of Telecommunications Standards, identified with the reference EN 319 411-2.

It guarantees the identity of the subscriber and the signatory, and a legal representation or power of attorney relationship between the signatory and an entity described in the "O" (Organization) field, and allows the generation of the "advanced electronic signature based on a qualified electronic certificate" .

Furthermore, this certificate can be used in other applications such as those listed below:

a) Authentication in access control systems.
b) Secure email signature.
c) Other electronic signature applications.

The usage information in the certificate profile indicates the following:

The "key usage" field has the following functions enabled and therefore allows us to perform them:

a. signature (to perform the authentication function)
b. Content commitment (to perform the electronic signature function)
c. Key Encipherment

1.1.35 Qualified Certificate of Natural Person Representative of an Entity without Legal Personality before the Administrations in QSCD

This certificate has the OID 1.3.6.1.4.1.4728 6.1.8.2.2 . It is a qualified certificate issued for qualified electronic signature and authentication, in accordance with the QCP-n - qscd certification policy with OID 0.4.0.194112.1.2, as stated in the certificate. This certificate , issued in QSCD, is a qualified certificate in accordance with Article 28 of Regulation (EU) 910/2014 eIDAS.

The certificate issued in QSCD works with qualified signature creation devices, in accordance with Articles 29 and 51 of Regulation (EU) 910/2014, and complies with the technical regulations of the European Telecommunications Standards Institute, identified by the reference EN 319 411-2 .

It guarantees the identity of the subscriber and the signatory, and a legal representation or power of attorney relationship between the signatory and an entity described in the "O" (Organization) field, and allows the generation of the "qualified electronic signature" that is, the advanced electronic signature that is based on a qualified certificate and that has been generated using a qualified device, which is equivalent to a written signature for legal effect, without the need to meet any other additional requirement.

It can also be used in applications that do not require an electronic signature equivalent to a written signature, such as the applications listed below:

a) Secure email signature.
b) Other electronic signature applications.

The usage information in the certificate profile indicates the following:

The "key usage" field has the following functions enabled and therefore allows us to perform them:

a. signature (to perform the authentication function)
b. Content commitment (to perform the electronic signature function)
c. Key Encipherment

1.1.36 Qualified certificate of natural person Representative of an Entity without Legal Personality before the administrations in centralized HSM

This certificate has the OID 1.3.6.1.4.1.472 86.1.8 .5. It is a qualified certificate issued for advanced electronic signature and authentication, in accordance with the QCP-n certification policy with the OID 0.4.0.194112.1.0.

It is a qualified certificate, in accordance with the provisions of Article 28 of Regulation (EU) 910/2014 eIDAS, and complies with the technical regulations of the European Institute of Telecommunications Standards, identified with the reference EN 319 411-2.

It guarantees the identity of the subscriber and the signatory, and a legal representation or power of attorney relationship between the signatory and an entity described in the "O" (Organization) field, and allows the generation of the "advanced electronic signature based on a qualified electronic certificate" .

Furthermore, the certificate can be used in other applications such as those listed below:

a) Authentication in access control systems.
b) Secure email signature.
c) Other electronic signature applications.

The usage information in the certificate profile indicates the following:

The “key usage” field has the following functions enabled and therefore allows us to perform them:

a. signature (to perform the authentication function)
b. Content commitment (to perform the electronic signature function)
c. Key Encipherment

1.1.37 Qualified certificate of natural person Representative of an Entity without Legal Personality before the administrations in centralized QSCD

This certificate has the OID 1.3.6.1.4.1.47286.1.8.6 . It is a qualified certificate issued for qualified electronic signature and authentication, in accordance with the QCP-n-qscd certification policy with OID 0.4.0.194112.1.2, as stated in the certificate. This certificate, issued in QSCD, is a qualified certificate in accordance with Article 28 of Regulation (EU) 910/2014 eIDAS.

The certificate issued in centralized QSCD works with qualified signature creation devices, in accordance with Articles 29 and 51 of Regulation (EU) 910/2014, and complies with the technical regulations of the European Institute of Telecommunications Standards, identified with the reference EN 319 411-2 .

It guarantees the identity of the subscriber and the signatory, and a legal representation or power of attorney relationship between the signatory and an entity described in the “O” (Organization) field, and allows the generation of the “qualified electronic signature” that is, the advanced electronic signature that is based on a qualified certificate and that has been generated using a qualified device, which is equivalent to a written signature for legal effect, without the need to meet any other additional requirement.

It can also be used in applications that do not require an electronic signature equivalent to a written signature, such as the applications listed below:

a) Secure email signature.
b) Other electronic signature applications.

The usage information in the certificate profile indicates the following:

The “key usage” field has the following functions enabled and therefore allows us to perform them:

a. signature (to perform the authentication function)
b. Content commitment (to perform the electronic signature function)
c. Key Encipherment

1.4. Certificate usage limits

1.4.1. Usage limits directed at signatories

The signatory must use the certificate certification service provided by UANATACA, exclusively for the uses authorized in the contract signed between UANATACA and the SUBSCRIBER, and which are reproduced below (section “obligations of the signatories”).

Furthermore, the signatory agrees to use the digital certification service in accordance with the instructions, manuals or procedures provided by UANATACA.

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

The signatory may not take any measures to inspect, alter or reverse engineer UANATACA's digital certification services without prior express permission.

1.4.2. Usage limits directed at verifiers

Certificates are used for their intended function and purpose, and cannot be used for other functions or purposes.

Similarly, certificates should only be used in accordance with applicable regulations, especially taking into account the import and export restrictions in place at any given time.

Certificates cannot be used to sign public key certificates of any kind, nor to sign certificate revocation lists (CRLs).

The certificates are not designed, cannot be intended for, and are not authorized for use or resale as equipment for controlling hazardous situations or for uses requiring fail-safe performance, such as the operation of nuclear facilities, air navigation or communications systems, or weapons control systems, where a failure could directly lead to death, personal injury, or severe environmental damage.

The limits indicated in the various fields of the certificate profiles, visible on the UANATACA website (https://www.uanataca.com), must be taken into account.

The use of digital certificates in operations that contravene this disclosure text, or the contracts with subscribers, is considered misuse for the appropriate legal purposes, therefore exempting UANATACA, according to current legislation, from any responsibility for this misuse of the certificates carried out by the signatory or any third party.

UANATACA does not have access to the data to which a certificate can be applied. Therefore, and as a consequence of this technical impossibility of accessing the message content, UANATACA cannot issue any assessment of said content. Consequently, the subscriber, signatory, or person responsible for its safekeeping assumes any liability arising from the content associated with the use of a certificate.

Likewise, the subscriber, the signatory, or the person responsible for custody will be liable. any liability that may arise from the use of the same outside the limits and conditions of use contained in this disclosure text, or in the contracts with the subscribers, as well as any other improper use of the same derived from this section or that may be interpreted as such according to the applicable regulations.

1.5. Subscriber Obligations

1.5.1. Key generation

The subscriber authorizes UANATACA to manage, in accordance with the appropriate methods and procedures, the issuance of the private and public keys for the signatories, and requests on their behalf the issuance of the certificate in accordance with UANATACA's certification policies.

1.5.2. Application for certificates

The subscriber undertakes to make applications for qualified certificates in accordance with the procedure and, if necessary, the technical components supplied by UANATACA, in accordance with what is set out in the certification practice statement (CPS) and in UANATACA's operations documentation.

1.5.3. Reporting obligations

The subscriber is responsible for ensuring that all information included in their certificate application is accurate, complete for the purpose of the certificate, and up-to-date at all times.

The subscriber must immediately inform UANATACA:

- Any inaccuracy detected in the certificate once it has been issued.
- Regarding changes that occur in the information provided and/or registered for the issuance of the certificate.
- From the loss, theft, misappropriation, or any other type of loss of control of the private key by the signatory.

1.6. Obligations of the signatories

1.6.1. Custodial obligations

The signatory undertakes to safeguard the personal identification code or any technical support provided by UANATACA, the private keys and, if necessary, the specifications owned by UANATACA that are supplied to him.

In the event of loss or theft of the certificate's private key, or if the signatory suspects that the private key has lost reliability for any reason, these circumstances must be reported immediately to the relevant Registration Authority or to UANATACA.

1.6.2. Obligations of proper use

The signatory must use the DCCF issued certificate certification service for individuals (QSCD) provided by UANATACA, exclusively for the uses authorized in the DPC and in any other instruction, manual or procedure supplied to the subscriber.

The signatory must comply with any laws and regulations that may affect their right to use the cryptographic tools employed.

The signatory may not take measures to inspect, alter or decompile the digital certification services provided.

The signatory will acknowledge:

a) That when you use any certificate, and as long as the certificate has not expired or been suspended or revoked, you will have accepted said certificate and it will be operational.

b) It does not act as a certification authority and, therefore, undertakes not to use the private keys corresponding to the public keys contained in the certificates for the purpose of signing any certificate.

c) In the event that the private key is compromised, you must immediately and permanently cease its use and proceed in accordance with this document.

1.7. Obligations of the verifier

1.7.1. Informed decision

UANATACA informs the verifier that they have access to sufficient information to make an informed decision when verifying a certificate and to trust the information contained in that certificate.

Additionally, the verifier will acknowledge that the use of the UANATACA Registry and Certificate Revocation Lists (hereinafter, "the CRLs" or "the CRLs") is governed by the UANATACA CPD and will commit to complying with the technical, operational, and security requirements described in said CPD.

1.7.2. Electronic signature verification requirements

The verification will normally be performed automatically by the verifier's software and, in any case, in accordance with the DPC, with the following requirements:

- It is necessary to use the appropriate software to verify an electronic signature with the algorithms and key lengths authorized in the certificate and/or to perform any other cryptographic operation, and to establish the certificate chain on which the electronic signature to be verified is based, since the electronic signature is verified using this certificate chain.
- It is necessary to ensure that the identified certificate chain is the most suitable for the electronic signature being verified, since an electronic signature can be based on more than one certificate chain, and it is the verifier's decision to ensure the use of the most suitable chain for verification.
- It is necessary to check the revocation status of the certificates in the chain with the information provided to the UANATACA Registry (with LRCs, for example) to determine the validity of all certificates in the certificate chain, since an electronic signature can only be considered correctly verified if each and every certificate in the chain is correct and valid.
- It is necessary to ensure that all certificates in the chain authorize the use of the private key by both the certificate subscriber and the signer, as some certificates may contain usage restrictions that would prevent trust in the verified electronic signature. Each certificate in the chain includes an indicator that refers to the applicable usage conditions, for review by the verifiers.
- It is necessary to technically verify the signature of all certificates in the chain before trusting the certificate used by the signer.

1.7.3. Trust in an unverified certificate

If the verifier relies on an unverified certificate, they will assume all the risks arising from this action.

1.7.4. Effect of verification

By virtue of the correct verification of the natural person certificates issued in DCCF (QSCD), in accordance with this disclosure text, the verifier can rely on the identification and, where applicable, public key of the signatory, within the corresponding limitations of use, to generate encrypted messages.

1.7.5. Proper use and prohibited activities

The verifier undertakes not to use any type of certificate status information or any other type of information that has been supplied by UANATACA, in carrying out any transaction prohibited by the law applicable to said transaction.

The verifier undertakes not to inspect, interfere with, or reverse engineer the technical implementation of UANATACA's public certification services without prior written consent.

Additionally, the verifier agrees not to intentionally compromise the security of UANATACA's public certification services.

The digital certification services provided by UANATACA have not been designed, nor are they permitted for use or resale, as equipment for controlling dangerous situations or for uses requiring fail-safe actions, such as the operation of nuclear facilities, air navigation or communication systems, air traffic control systems, or weapons control systems, where an error could cause death, physical harm, or serious environmental damage.

1.7.6. Indemnity clause

The third party relying on the certificate agrees to indemnify and hold harmless UANATACA from any and all damages arising from any action or omission that results in liability, damage or loss, expenses of any kind, including legal and representation costs that may be incurred, due to the publication and use of the certificate, when any of the following causes occur:

- Failure to comply with the obligations of the third party that relies on the certificate.
- Reckless reliance on a certificate, given the circumstances.
- Failure to verify the status of a certificate to determine that it is not suspended or revoked.
- Failure to verify all the security measures prescribed in the DCP or other applicable regulations.

1.8. UANATACA's Obligations

1.8.1. Regarding the provision of the digital certification service

UANATACA undertakes to:

a) Issue, deliver, manage, suspend, reactivate, revoke and renew certificates, in accordance with the instructions provided by the subscriber and/or signatory, in the cases and for the reasons described in the UANATACA DPC.

b) Perform the services with the appropriate technical and material means, and with personnel who meet the qualification and experience conditions established in the DPC.

c) To meet the quality levels of service, in accordance with what is established in the DPC, in the technical, operational and security aspects.

d) Notify the subscriber and the signatory, prior to the expiration date of the certificates, of the possibility of renewing them, as well as the suspension, lifting of this suspension or revocation of the certificates, when such circumstances occur.

e) Communicate to third parties who request it, the status of the certificates, in accordance with what is established in the DPC for the different certificate verification services.

1.8.2. Regarding the registration checks

UANATACA is obligated to issue certificates based on the data provided by the subscriber, and may therefore carry out the checks it deems appropriate regarding the identity and other personal and supplementary information of the subscribers and, when appropriate, of the signatories.

These checks may include the supporting documentation provided, and any other relevant documents and information provided by the subscriber and/or signatory.

If UANATACA detects errors in the data to be included in the certificates or in the supporting documentation, it may make the necessary changes before issuing the certificate or suspend the issuance process and address the issue with the subscriber. If UANATACA corrects the data without first addressing the issue with the subscriber, it must notify the subscriber of the final certified data.

UANATACA reserves the right not to issue the certificate when it considers that the documentary justification is insufficient for the correct identification and authentication of the subscriber and/or the signatory.

The above obligations will be suspended in cases where the subscriber acts as a registration authority and has the technical elements corresponding to the generation of keys, issuance of certificates and recording of corporate signature devices.

1.8.3. Preservation periods

UANATACA archives records related to applications for issuance and revocation of certificates for at least 15 years.

UANATACA stores log information for a period of between 1 and 15 years, depending on the type of information recorded, in accordance with its policies and procedures.

1.9. Limited warranties and warranty disclaimers

1.9.1. UANATACA's guarantee for digital certification services

UANATACA guarantees the subscriber:

- That there are no factual errors in the information contained in the certificates, known or made by the Certification Authority.
- That there are no factual errors in the information contained in the certificates, due to a lack of due diligence in the handling of the certificate application or in the creation of the certificate.
- That the certificates meet all the material requirements established in the DPC.
- That the revocation services and the use of the deposit comply with all the material requirements established in the DPC.

UANATACA guarantees to the third party that relies on the certificate:

- That the information contained or incorporated by reference in the certificate is correct, except where otherwise indicated.
- In the case of certificates published in the deposit, that the certificate has been issued to the subscriber and signatory identified therein and that the certificate has been accepted.
- That in the approval of the certificate application and in the issuance of the certificate, all the material requirements established in the DPC have been met.
- Speed and security in the provision of services, especially revocation and deposit services.

Additionally, UANATACA guarantees to the subscriber and to the third party that relies on the certificate:

- That the qualified certificate for signature contains the information that a qualified certificate must contain, in accordance with the provisions of Article 28 of Regulation (EU) 910/2014, complying with the provisions of the technical regulations identified with the reference ETSI EN 319 411-2.
- That, in the event that it generates the private keys of the subscriber or, where applicable, the natural person identified in the certificate, their confidentiality is maintained during the process.
- The Certification Authority's responsibility is subject to the limits established. In no case will UANATACA be liable for acts of God or force majeure.

1.9.2. Warranty Exclusion

UANATACA rejects any other guarantee other than the one above that is not legally enforceable.

Specifically, UANATACA does not guarantee any software used by any person to sign, verify signatures, encrypt, decrypt, or otherwise use any digital certificate issued by UANATACA, except where there is a written statement to the contrary.

1.10. Applicable Agreements and DPC

1.10.1. Applicable agreements

The agreements applicable to the certificates are as follows:

- Certification services contract, which regulates the relationship between UANATACA and the subscriber of the certificates.
- General terms and conditions of service incorporated in this document.
- Statement of Certification Practices, which regulate the issuance and use of certificates.

1.10.2. Certification Practice Statement

UANATACA's trusted services are regulated technically and operationally by UANATACA's Certification Practice Statement (CPS), its subsequent updates, and supplementary documentation.

The DPC and the documentation of operations are periodically updated in the Registry and can be consulted on the website: https://www.uanataca.com .

1.11. Rules of trust for long-established firms

UANATACA informs applicants for certificates that it does not offer a service that guarantees the reliability of an electronic signature of a document over time.

1.12. Privacy policy

UANATACA cannot disclose, nor can it be compelled to disclose, any confidential information regarding certificates without a specific prior request from:

a) The person with respect to whom UANATACA has a duty to keep information confidential, or

b) A court order, an administrative order, or any other order provided for in current legislation.

However, the subscriber agrees that certain personal and other information provided in the certificate application may be included in their certificates and in the certificate status verification mechanism, and that the aforementioned information is not confidential, as required by law.

UANATACA does not share with any person the data provided specifically for the provision of the certification service.

1.13. Privacy Policy

UANATACA has a privacy policy in section 9.4 of the DPC, and specific privacy regulations in relation to the registration process, the confidentiality of the registration, the protection of access to personal information, and the user's consent.

It is also stipulated that the supporting documentation for the approval of the application must be kept and duly registered with security and integrity guarantees for a period of 15 years from the expiration of the certificate, even in the event of early loss of validity due to revocation.

1.14. Refund policy

UANATACA will not refund the cost of the certification service under any circumstances.

1.15. Applicable regulations and competent jurisdiction

Relations with UANATACA will be governed by the provisions of Regulation (EU) 910/2014 eIDAS, by Spanish laws, and, in particular, by all those derived from its compliance policy.

The competent jurisdiction is that indicated in Law 1/2000, of January 7, on Civil Procedure.

1.16. Linkage with the list of Qualified Providers of Trusted Electronic Services

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

1.17. Divisibility of clauses, survival, full agreement and notification

The clauses in this disclosure text are independent of each other, which is why, if any clause is considered invalid or unenforceable, the remaining clauses of the PDS will continue to apply, unless expressly agreed otherwise by the parties.

The requirements contained in sections 9.6.1 (Obligations and Responsibilities), 8 (Compliance Audit) and 9.3 (Confidentiality) of the UANATACA DPC will continue to be in effect after the termination of service under the terms provided therein.

This text contains the full intent and all agreements between the parties.

The parties notify each other of facts by means of an email procedure to the following addresses:

- info@uanataca.com, on behalf of UANATACA
- The email address, indicated by the subscriber in the contract with UANATACA.