



PKI Disclosure Statement

Policy for Qualified Electronic Signature and for
Qualified Electronic Seal



INDICE

GENERAL INFORMATION.....	3
Documentary Check.....	3
Formal Control.....	3
Version Control.....	3
1. Disclosure statement.....	4
1.1. Introduction.....	4
1.2. Document name and identification.....	4
1.3. Contact Information.....	4
1.3.1. Organization.....	4
1.3.2. Certificate issuing.....	5
1.3.3. Revocation proceedings contact.....	5
1.4. Certificates Type.....	5
1.5. Purpose of the certificates.....	6
1.5.1. Common provision.....	6
1.5.2. Qualified certificate issued for Qualified Electronic Signature.....	6
.....	7
1.5.3. Qualified certificate signature of 'One-Shot' type.....	7
1.5.4. Qualified certificate of legal person seal in QSCD.....	7
1.6. Limitations and restrictions on certificate usage.....	8
1.6.1. Limitation for certificate holders.....	8
1.6.2. Subscribers obligations.....	8
1.7. Key generation.....	9
1.8. Certificates request.....	9
1.9. Subscribers obligations.....	9
1.10. Certificate-holder obligations.....	9
1.10.1. Custody obligations.....	9
1.10.2. Obligations of proper use.....	9
1.11. Relying Parties Obligations.....	10
1.11.1. Informed decision.....	10
1.11.2. Elected signature and seal verification requirements.....	10
1.11.3. Trusting a certificate not verified.....	11
1.11.4. Verification effect.....	11
1.11.5. Proper use and prohibited activity.....	11
1.11.6. Indemnity clause.....	11

1.12.	Uanataca S.A. obligations	11
1.12.1.	Digital certification services provision.....	11
1.12.2.	Regarding the registry check	12
1.12.3.	Retention period.....	12
1.13.	Guarranty.....	12
1.13.1.	Uanataca S.A. guarantees for certification services	12
1.14.	Guarantee exclusion.....	13
2.	APPLICABLE AGREEMENTS.....	14
2.1.	Applicable agreements	14
2.2.	Certification Practice Statement (CPS)	14
2.3.	Privacy Policy	14
2.4.	Refund policy.....	15
2.5.	Applicable law and jurisdiction	15
2.6.	List of active trust service provider	15
2.7.	Final provisions, full agreement and notifications	15

GENERAL INFORMATION

Documentary Check

Security Classification:	Public
Organization:	Uanataca S.A. unipersonal
Version:	1.3
Last Edition Date:	16/06/2022
Document code:	PKI_Disclosure_Statement_v.1.3_EN

Formal Control

Prepared by:	Revised by:	Approved by:
<i>Legal & Compliance</i>	<i>Legal & Compliance</i>	<i>Direction</i>

Version Control

Version	Modified parts	Changelog	Date
1.0	Original	File Creation	31/03/2020
1.1	Structure and formatting of the document	Normative references added, new logo added, formatting adaption	01/12/2020
1.2	Entire document	Paragraph formatting update	20/05/2021
1.3	Par. 1.4, 1.5.2, 1.5.3, 1.5.4, 2.1	Update of Certificate Types/OID and introduction of 'One-shot' Certificate issuing flow	16/06/2022

1. Disclosure statement

1.1. Introduction

This PKI Disclosure Statement document (hereinafter also just "*Statement*"), drawn up in accordance with ETSI EN 319 411-1, is part of the Uanataca S.A. unipersonal (hereinafter also just "*Uanataca*") terms and conditions which relate to the operation of the PKI.

This Statement prepared in accordance with the "*PDS structure*" referred to in letter A2 of Annex A contained in the ETSI standard mentioned above contains the essential information to be known in relation to the certification services of the Qualified Trust Service Provider Uanataca.

For all the terms and definitions used within this document, it is possible to refer to the Uanataca CPS (*Certification Practice Statement*) available at <https://web.uanataca.com/it/politiche-di-certificazione> or to the definitions provided by the applicable legislation.

1.2. Document name and identification

This document is updated to the version resulting from the "*Version Control*" or "*Documentary Check*" referred to in the "*General Information*" of this Statement.

Uanataca ensures constant verification and constant updating of the document that takes into account any subsequent regulatory updates.

Furthermore, Uanataca undertakes to make this document known and available to interested parties by publishing it on its website where it is always possible to consult the latest approved version.

1.3. Contact Information

1.3.1. Organization

Below are the company data of Uanataca S.A. unipersonal and related contacts:

UANATACA S.A. UNIPERSONAL

Legale office: Calle Riera de Can Todà 24-26 - Barcellona

Italy branch: Via Diocleziano n. 107, 80125 - Naples

Vat Number (ES): A66721499

Vat Number (IT): 09156101215

Phone: +39 081 7625600

E-mail: info.it@uanataca.com

Web Site: <https://web.uanataca.com/it/>

1.3.2. Certificate issuing

The certificates described in this document are issued by Uanataca, as mention previously (v.1.3.1. *infra*).

1.3.3. Revocation proceedings contact

For requests for certificate revocation, Holders and interested parties can contact Uanataca by communicating to one of the contacts indicated below (for the revocation the provisions of the CPS apply.:

UANATACA S.A. UNIPERSONALE
Telephone: +39 081 7625600
E-mail: info.it@uanataca.com

1.4. Certificates Type

The certificates issued by Uanataca are qualified in compliance with articles 28 and 38 as well as Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 (hereinafter also only "eIDAS Regulation") and comply with the provisions of the technical reference standard ETSI EN 319 411-1 / 2 in its latest approved versions.

The Objective Identifier (OID) identifying the Uanataca CA is the following:

1.3.6.1.4.1.47286

Uanataca, in addition, has assigned each type of certificate an object identifier (OID), as specified below:

OID number	Kind of certificate
	Electronic signature service
1.3.6.1.4.1.47286.10.1.1	Qualified certificate of subscription in QSCD device
1.3.6.1.4.1.47286.10.1.2	Qualified certificate of subscription in QSCD remote device
1.3.6.1.4.1.47286.10.1.3	Qualified certificate of subscription of 'One-shot' type in QSCD remote device
1.3.6.1.4.1.47286.10.1.10	Qualified certificate of electronic seal in QSCD device
1.3.6.1.4.1.47286.10.1.11	Qualified certificate of electronic seal in QSCD remote device
	CNS issuing service

1.3.6.1.4.1.47286.10.3.1	Authentication certificate
--------------------------	----------------------------

Uanataca undertakes, for each type of qualified certificate issued, to make the CRL (Certificate Revocation List) available for the entire period of validity of the certificates in accordance with point 6.3.10-02 of ETSI 319 411-2.

1.5. Purpose of the certificates

1.5.1. Common provision

The qualified certificates described in this document guarantee the certificate holder identity allowing the generation of the "*qualified electronic signature*" and the "*qualified electronic seal*".

The aforementioned certificates, issued in QSCD (on Smartcard/Token or HSM – Remote Signature), operate with qualified signature creation devices, in accordance with the eIDAS Regulation and in compliance with the technical regulations of the European Telecommunications Standards Institute EN 319 411-2 mentioned above.

1.5.2. Qualified certificate issued for Qualified Electronic Signature

These certificates are identified by the OIDs referred to in Section 1.4 of this document. They are qualified certificates issued for qualified electronic signature that, both in the case of issuance on Smartcard/Token (see Par. 4.3.1.1. of the CPS) and in the case of issuance on HSM (see Par. 4.3.1.2. of the CPS) comply with certification policy QCP-n-qscd with OID 0.4.0.194112.1.2, which is declared in the certificates.

These certificates, issued in QSCD constitute qualified certificates in accordance with Article 28 of Regulation (EU) 910/2014 eIDAS.

They operate with qualified signature-creation devices (QSCD), in compliance with Articles 29 and 51 of Regulation (EU) 910/2014, and in accordance with the provisions of the technical regulation issued by the European Telecommunications Standards Institute, identified by reference EN 319 411-2.

Furthermore, they guarantee the identity of the Holder and enable the generation of a 'qualified electronic signature', i.e., an advanced electronic signature based on a qualified certificate and generated using a qualified device, which is equated, for all legal purposes, with a handwritten signature without the need for any further requirements.

Furthermore, the certificate in question can be used for those applications that do not require an electronic signature equivalent to a written signature, such as

- a. Secure e-mail signature;
- b. Other electronic signature applications.

The '*key usage*' field only allows for the '*content commitment*' function (non-repudiation).

1.5.3. Qualified certificate signature of 'One-Shot' type

This is a qualified signature certificate issued on an HSM (remote signature) device with a more limited period of validity, typically not exceeding 60 days or as otherwise agreed with the customer/third party concerned and, in any case, with a duration of use not exceeding 60 minutes from the issue of the certificate. In addition, its use is permitted by means of authentication systems permitted by law and only in the manner and under the terms of the limitations of use included in the certificate, established by Uanataca and accepted by the Holder when requesting the certificate issue.

In conjunction with the affixing of the signature, a time stamp is also inserted to guarantee a certain time reference in accordance with the regulations.

For this type of certificate, there is no provision for revocation or suspension. There is a specific usage limit, to be agreed with the customer. For the limits of use, please refer to paragraph 4.5.3. of the CPS.

1.5.4. Qualified certificate of legal person seal in QSCD

These certificates are marked with OID 1.3.6.1.4.1.47286.10.1.10 for issuance on Smartcard/Token and OID 1.3.6.1.4.1.47286.10.1.11 for issuance on HSM (remote seal) respectively. These are qualified certificates issued for the qualified electronic seal, in accordance with certification policy QCP-I-qscd with OID 0.4.0.194112.1.3, which is declared in the certificates.

Such certificates, issued in "Qualified Seal Creation Device" (hereinafter also only "QSealCD" or also "QSCD", constitute qualified certificates within the meaning of Article 38 of Regulation (EU) 910/2014 eIDAS: "Qualified Electronic Seal Certificates".

They operate with qualified signature-creation devices and electronic seals (QSCD), in compliance with Articles 39 and 51 of Regulation (EU) 910/2014, and in accordance with the provisions of the technical regulation issued by the European Telecommunications Standards Institute, identified by reference EN 319 411-2.

In addition, it guarantees full legal validity and traceability to a specific legal entity (Holder) and makes it possible to generate a 'qualified electronic seal', which is equated, for all legal purposes, to a signature in written form without the need for further requirements.

The qualified electronic seal, in fact, enjoys the presumption of the integrity of the data and the correctness of the origins of such data, to which the qualified electronic seal is linked, and provides full proof of the issuance of the document by a legal person, guaranteeing the certainty of the origin and integrity of the document.

The "key usage" field only allows for the "content commitment" function (non-repudiation).

1.6. Limitations and restrictions on certificate usage

1.6.1. Limitation for certificate holders

The Holder must use the certificate certification service provided by Uanataca exclusively in compliance with the provisions of the CPS published on the organization's website at the following address <https://web.uanataca.com/it/politiche-di-certificazione> and in any case, for the uses authorized in the contract signed between Uanataca and the Holder.

For more information, the Holder is invited to consult the general terms and conditions of the certification services contract, available at the following link: <https://web.uanataca.com/it/condizioni-general-del-servizio>.

Likewise, the Holder undertakes to use the digital certification service in accordance with the instructions, manuals or procedures provided by Uanataca.

The Holder must comply with any legislation and regulations that may affect his right to use the cryptographic tools he uses.

The certificates can only be used for the functions and purposes established by the Uanataca CPS and by any Terms and Conditions signed by Subscribers at the time of requesting the certificate without expressly exclusion of any other use.

As a result, certificates cannot be used to sign public key certificates of any kind, nor can they sign certificate revocation lists (CRLs).

This is without prejudice to compliance with the applicable legislation for the use of certificates.

They must also take into account the limits indicated in the various fields of the certificate profiles visible on the Uanataca website (<https://web.uanataca.com/it/>).

In case of use of the certificates in violation of the provisions contained in this Policy or in violation of the provisions mentioned above, the user will be required to release Uanataca from any liability that may arise in relation to the illegitimate use of the certificates in accordance with current legislation.

Uanataca undertakes to keep the following information on registration certificates for a period of 20 (twenty) years, in accordance with applicable legislation:

- information on the subjects relating to the identification and registration procedures;
- information on the life cycle of certificates;
- significant event logs for security purposes.

Further information on conservation are indicated in the following paragraphs.

1.6.2. Subscribers obligations

The Subscribers, or those who request the issue of a qualified certificate in Uanataca, are required to comply with the provisions of this Policy, the CPS manual, the Terms and Conditions accepted

at the conclusion of the contract and any other rules established by the CA, which are adequately and publicly made available to applicants.

1.7. Key generation

The subscriber authorizes Uanataka to generate the relevant methods and procedures, the issue of private and public keys for the signers and request on behalf the issuance, the issue of the certificate in accordance to the certification policies of Uanataka.

1.8. Certificates request

The Subscriber undertakes to request the qualified certificates in accordance with the procedure and, if necessary, the technical components supplied by Uanataka, in accordance with what is established in the certification practice statement (CPS) and Uanataka operations documentation.

1.9. Subscribers obligations

The subscriber is responsible for all information included in the application for the certificate is accurate, complete for the purpose of the certificate and updated at all times.

The subscriber must immediately inform Uanataka of:

- any inaccuracies detected in the certificate once issued;
- The changes that occur in the information provided and/or registered to issue the certificate;
- The loss, theft, subtraction, or any other type of control loss of the private key by the signer.

In addition, the subscriber is required to verify the date indicated in the certificate.

1.10. Certificate-holder obligations

1.10.1. Custody obligations

The signer binds to custody the personal identification code or any other technical support delivered to Uanataka, the private keys and, if necessary, Uanataka properties specifications that are supplied.

In case of loss or theft of the certificate private key, or if the signer suspects that the private key has lost reliability for any reason, such circumstances must be notified immediately to Uanataka by the Subscriber.

1.10.2. Obligations of proper use

The signer must use qualified digital certificates provided by Uanataka, only for authorized uses in the CPS and in any other instruction, manual or procedure provided at the time of the application for the issue and on the website <https://web.uanataka.com/it/politiche-di-certificazione>.

The signer must comply any law and regulation that may affect their right of use the cryptographic tools used.

The signer won't be able to adopt the inspection, alteration or decompiling measures of the digital certification services provided.

The signer also undertakes:

- a) to comply with the above provisions about the use of the certificate;
- b) in the event of any compromise of the private key, to immediately and permanently discontinue its use and make the appropriate notifications set forth in this document.

1.11. Relying Parties Obligations

1.11.1. Informed decision

Uanataca informs the Relying Parties that has access to enough information to make an informed decision when verifying a certificate and rely on the information contained in that certificate.

In addition, the Relying Parties will recognize that the use of the Registry and the Certificates Revocation Lists (hereinafter "the CRLs") of Uanataca are governed by the CPS of Uanataca and will compromise to comply the technical, operational and security requirements, described in the mentioned CPS.

1.11.2. Electronic signature and seal verification requirements

The verification will normally be performed automatically by the verification software and, in any case, in accordance with the CPS manual with the following requirements:

- it is necessary to use appropriate software for verification, capable of performing the necessary cryptographic operations using algorithms and key lengths indicated in the certificate;
- it is necessary to verify the revocation status of the certificates of the "trust" chain with the information provided to the Uanataca Registry (with CRL for example) to determine the validity of all the certificates in the chain of certificates, since it can only be considered properly verified an electronic signature if all and each of the certificates in the chain are correct and are in force;
- it is necessary to technically verify the signature of all the certificates in the chain before ascertaining the certificate used by the signatory.

Uanataca makes available to the *Relying Parties* an application (can be reached at the following address: <https://vol.uanataca.com/it>) that allows the verification of qualified certificates of signature and electronic seal: this application and the relative procedure is indicated and described in Annex A to the Uanataca CPS.

1.11.3. Trusting a certificate not verified

Uanataka cannot, in any case, be held liable in the event that the Relying Parties consider an invalid certificate to be trustworthy; in such an event, in fact, they will assume all risks derived from such behavior.

1.11.4. Verification effect

Under proper verification of natural person certificate issued on QSCD, in accordance with this disclosure text, the *Relying Parties* can rely on the identification and, where appropriate, on the signer's public key, within the limitations of appropriate use, to generate encrypted messages.

1.11.5. Proper use and prohibited activity

The Relying Parties undertake not to use any information relating to the certificates or of any other type that has been provided by Uanataka in carrying out transactions prohibited by law.

The digital certification services provided by Uanataka have not been designed nor allow their use or resale as control equipment for unauthorized dangerous situations or for uses that require actions subject to error, such as the operations of nuclear installations, navigation systems, air communication or arms control systems, where an error could cause death, physical harm or serious environmental damage.

1.11.6. Indemnity clause

The *Relying Party* agrees to indemnify Uanataka S.A. of any damage from any action or omission that results in liability, damage or loss, expenses of any kind, including court and legal representation that may be incurred by the publication and use of the certificate, when any of the following causes occurs:

- Breach of the obligations of the relying party in the certificate.
- Reckless confidence in a certificate, along with the circumstances.
- Lack of checking of the certificate status, to determine that it is not suspended or revoked.
- Lack of checking of all security measures prescribed in the CPS or other applicable regulations.

1.12. Uanataka S.A. obligations

1.12.1. Digital certification services provision

Uanataka undertakes to:

- a. Issue, deliver, manage, suspend, revoke and renew certificates, according to the instructions provided by the subscriber, in the cases and for the reasons described in Uanataka CPS.

- b. Perform the services with technical media and suitable materials, and with personnel that meet the qualification conditions and experience established in the CPS.
- c. Comply the quality service levels, in accordance with what is established in the CPS, in the technical, operational and security aspects.
- d. Notify the subscriber, prior the certificates expiration date, the possibility of renewal and suspension, lifting of this suspension or revocation of certificates, when such circumstances occur.
- e. Communicate to third parties who request the status of certificates, according to what is established in the CPS for different certificate verification services.

1.12.2. Regarding the registry check

Uanataka will issue the certificates on the basis of the data and information provided by the Subscribers: for this purpose, it has adopted a rigid procedure for identifying the applicants, in accordance with current legislation, accurately described in the CPS, with which it will carry out the checks it deems appropriate for the verification of the identity and other personal and complementary information of the Subscribers and Holders.

These checks may include any other relevant documents and information provided by the Subscriber and / or the Holders.

In the event that Uanataka finds errors in the data that must be included in the certificates, before issuing the certificate or suspending the issuing process, it will be able to make the changes it deems necessary only after managing the case with the Subscriber.

Uanataka reserves the right not to issue the certificate if it considers that the documentary justification is insufficient for the correct identification and authentication of the Subscriber and / or Holders.

The previous obligations are suspended in cases where the subscriber acts as a registration authority and has the technical elements inherent in the generation of keys, the issue of certificates and the registration of company signature devices.

1.12.3. Retention period

We can archive requests for issuing and revoking certificates for at least 20 years.

Uanataka will retain the information in the registers for a period of between 1 and 20 years depending on the type of information registered as required by the policies and procedures.

For more information on retention periods, please consult the CPS.

1.13. Guarranty

1.13.1. Uanataka S.A. guarantees for certification services

Uanataka guarantees to the Subscribers/ Holders:

- that there are not factual errors in the information in the certificates, known or made by the Certification Authority.
- that there are not factual errors in the information in the certificates, due to lack of diligence due to the management of the certificate request or creation of it.
- that the certificates comply with the material requirements established in the CPS.
- that the revocation services and the use of the deposit comply with all material requirements established in the CPS.

Uanataka guarantees to the *Relying Parties*:

- that the information contained or incorporated by reference in the certificate is accurate, except where indicated the opposite.
- in case of certificates published in the deposit, the certificate has been issued to the Subscriber identified in it and the certificate has been accepted.
- that in the approval of the certificate request and in the certificate issuance all the material required established in the CPS has been accomplished.
- the rapidity and security in the certification services provision, especially in the revocation services and Deposit.

In addition, guarantees to the Subscribers and the *Relying Party*:

- that the signature and seal qualified certificate contains the information that a qualified certificate must have, in accordance with Article 28 and 38 of the Regulation (UE) 910/2014, in compliance with the technical regulation identified with reference ETSI EN 319 411-2;
- that, in case of private keys generated by the Subscribers or, where appropriate, the natural person identified on the certificate, his confidentiality is preserved during the process;
- the responsibility of the Certification Authority, with the limits established.

Under no circumstances will Uanataka be liable for unforeseeable circumstances or force majeure.

1.14. Guarantee exclusion

Uanataka rejects any other different guarantee to the previous that is not legally enforceable. Specifically, Uanataka does not guarantee any software used by anyone to sign, verify signatures, encrypt, decrypt, or use any digital certificate in any other way issued by Uanataka, except in cases where a written declaration to the contrary exists.

2. APPLICABLE AGREEMENTS

2.1. *Applicable agreements*

Applicable agreements to the certificates are the followings:

- General Terms and Conditions for Digital Certification Services governing the relationship between Uanataca and the Applicant/Certificate Holder available at: <https://web.uanataca.com/it/condizioni-general-del-servizio>;
- Service general terms and information incorporated in this disclosure text;
- CPS governing the provision of certification services (see section 2.2. below);
- Any additional forms and/or contractual documentation expressly referred to in the above documents.

2.2. *Certification Practice Statement (CPS)*

Uanataca certification services are technically an operationally regulated by the CPS of Uanataca, for its subsequent updates, as well as the additional documents.

The CPS and the operations documentation are changed periodically in the Registry and can be consulted on the website: <https://web.uanataca.com/it/politiche-di-certificazione>.

2.3. *Privacy Policy*

Uanataca, with reference to the processing of personal data, complies with current legislation, both national and community, with particular reference to Legislative Decree 196/03, as amended, and Regulation (EU) 2016/679 (hereinafter also referred to as "GDPR").

Uanataca cannot disclose or be obliged to disclose confidential information unless a specific request comes from:

- a) the person with whom Uanataca has an obligation to keep the information confidential,
or
- b) a judicial, administrative or any other mandate provided for by current legislation.

However, the subscriber accepts that certain personal or other information, provided in the certificate request, is included in the certificates and in the certificate status verification mechanism, and that the information mentioned is not confidential by law.

Uanataca, in accordance with the provisions of art. 13 of the GDPR, has prepared and adopted a precise Privacy Policy relating to the registration process, the confidentiality of the registration, the protection of access to personal information and the user's consent.

The information in extended format is available in the Uanataca CPS: <https://web.uanataca.com/it/politiche-di-certificazione>.

2.4. Refund policy

For the refund policy it is necessary to refer to the relative section in the Uanataca CPS.

2.5. Applicable law and jurisdiction

Relations with Uanataca are governed exclusively by the Italian law.

In the event of disagreement between the parties, they will attempt amicable settlement. To this end, the parties must send a communication to Uanataca through one of the contacts indicated in this document.

For the competent court, please refer to the Uanataca CPS, which is to be understood here as fully referred to and transcribed.

2.6. List of active trust service provider

Below is the link through which it is possible to consult the list of active trust service providers in Italy: <https://www.agid.gov.it/it/piattaforme/firma-elettronica-qualificata/prestatori-di-servizi-fiduciari-attivi-in-italia>

2.7. Final provisions, full agreement and notifications

The clauses of this disclosure text are independent of each other, that's why, if any clause is held invalid or unenforceable, the remaining clauses of this Policy will still be applicable, except expressly agreed by the parties.

The requirements contained in sections 9.6.1 (Obligations and liability), 8 (audit of conformity) and 9.3 (Confidentiality) of the CPS of Uanataca shall continue in force after the service termination.

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

The parties mutually notify the facts by sending an email to the address indicated by the subscriber in the contract with Uanataca.



Bringing trust and simplicity into the digital future



www.uanataca.com

