PKI Disclosure Statement (PDS) - Qualified Electronic Time-Stamping Authority (TSA)PKI Disclosure Statement (PDS) - Qualified Electronic Time-Stamping Authority (TSA)



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-3.3**	**UANATACA, S.A.**
Edited by	**Alejandro Grande**	Classification	**Public**	Legal Representative
Verified by	**AGR**	Version	**3.1**	**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. Contact information 2

1.1. Responsible organization 2

1.2. Contact 3

1.3. Contact for revocation processes 3

2. Type and purpose of the certificate 3

2.1. Issuing Certification Entity 4

3. Certificate usage limits 4

3.1. Issuing Certification Entity 4

3.2. Usage limits directed at verifiers 5

4. Subscriber Obligations 5

4.1. Key generation 5

4.2. Application for certificates 5

4.3. Reporting obligations 5

4.4. Custodial obligations 6

4.5. Obligations of proper use 6

4.6. Prohibited transactions 7

5. Obligations of the verifiers 7

5.1. Informed decision 7

5.2. Timestamp verification requirements 8

5.3. Trust in an unverified certificate 9

5.4. Proper use and prohibited activities 9

5.5. Indemnity clause 9

6. UANATACA 's Obligations 10

6.1. Regarding the provision of digital certification 10

6.2. Regarding the registration checks 11

6.3. Preservation periods 11
7. Limited warranties and warranty disclaimers 11
7.1. UANATACA's guarantee for digital certification services 11
7.2. Warranty Exclusion 13
8. Agreements and policies 13
8.1. Applicable agreements 13
8.2. DPC 14
8.3. Privacy policy 14
8.4. Privacy Policy 15
8.5. Refund policy 15
8.6. Applicable law and competent jurisdiction 15
8.7. Accreditations and quality seals 16
8.8. Link to the list of providers 16
8.9. Divisibility of clauses, survival, full agreement and notification 16

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	DMP	23/06/2017
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	Complete	Adaptation of the document to the new corporate formats. Modification of the certificate profiles to which this PDS applies.	AGB	30/03/2026
3.1	Complete change	Adaptation to Namirial corporate formats due to change of company name	Alejandro Grande	23/10/2026

POPULARIZATION TEXT APPLICABLE TO THE ELECTRONIC TIME-STAMPING AUTHORITY QUALIFIED ELECTRONIC SEAL CERTIFICATE

This document contains the essential information to know regarding the certification service of the UANATACA Certification Entity.

This document follows the structure defined in Annex A of the ETSI EN 319 411-1 standard, in accordance with the indications of section 4.3.4 of the ETSI EN 319 412-5 standard.

1. Contact information

1.1. Responsible organization

The UANATACA Certification Entity, hereinafter “UANATACA”, is an initiative of:

UANATACA, SA

MERIDIANA AVENUE, 350, 3RD FLOOR, 08027 BARCELONA

TELEPHONE: 935 272 290

EMAIL: INFO@UANATACA.COM

1.2. Contact

For any inquiries, please contact:

UANATACA, SA

MERIDIANA AVENUE, 350, 3RD FLOOR, 08027 BARCELONA

TELEPHONE: 935 272 290

EMAIL: INFO@UANATACA.COM

1.3. Contact for revocation processes

For any inquiries, please contact:

UANATACA, SA

MERIDIANA AVENUE, 350, 3RD FLOOR, 08027 BARCELONA

TELEPHONE: 935 272 290

EMAIL: INFO@UANATACA.COM

2. Type and purpose of the certificate

This certificate has the following OID:

1.3.6.1.4.1.47286.1.5	According to the UANATACA hierarchy
0.4.0.194112.1. 3	In accordance with EU policy (QCP-l-qscd)

Electronic Time Stamping Authority certificates are qualified certificates in accordance with Article 38 and Annex III of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical standards identified with the references ETSI EN 319 412-3, ETSI EN 319 421 and ETSI EN 319 422.

These certificates allow the signing of digital evidence of electronic time.

The usage information in the certificate profile indicates the following:

a) The “key usage” field has the following functions enabled, and therefore allows us to perform them:
    a. Electronic Signature
    b. Content commitment (to perform the electronic signature function)
b) The following indication is available in the “extKeyUsage” field by default:
    a. “timeStamping” to perform the electronic timestamping function.
c) The “User Notice” field describes the use of this certificate.

2.1. Issuing Certification Entity

These certificates are issued by UANATACA, identified by the data indicated above.

3. Certificate usage limits

3.1. Issuing Certification Entity

The qualified electronic time stamping 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”).

The electronic timestamping service must be used in accordance with the instructions, manuals or procedures supplied by UANATACA.

Any laws and regulations that may affect the use of the tools must be complied with. cryptographics that it uses.

Inspection, alteration, or reverse engineering measures cannot be adopted on the UANATACA electronic time-stamping services, without prior express permission.

3.2. Usage limits directed at verifiers

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

to be employed in other functions and for other purposes.

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

applicable, especially taking into account import restrictions and

exports existing at any given time.

4. Subscriber Obligations

4.1. Key generation

The subscriber authorizes UANATACA to generate the private and public keys for the issuance of this certificate.

4.2. Application for certificates

The subscriber undertakes to make the requests, when necessary, for these certificates in accordance with the procedure and, if necessary, the technical components supplied by UANATACA, in accordance with what is established in the certification practice statement (CPS) and in the UANATACA operations documentation.

4.3. 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 custodian.

4.4. Custodial obligations

The subscriber undertakes to safeguard all information generated in its activity as a registration entity.

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 you.

In case of loss or theft of the certificate's private key, or if it is suspected that the private key has lost reliability for any reason, these circumstances must be reported immediately to UANATACA through the subscriber.

4.5. Obligations of proper use

The certificate must be used exclusively for the uses authorized in the DPC and any other instruction, manual, or procedure supplied to the subscriber.

You must comply with any laws and regulations that may affect your right to use the cryptographic tools employed.

Inspection, alteration or decompilation of the digital certification services provided may not be carried out.

Besides:

a) When any certificate is used, and as long as the certificate has not expired, been suspended, or been revoked, the certificate will be considered accepted and operational.

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

c) If the private key is compromised, its use is immediately and permanently suspended.

4.6. Prohibited transactions

It is indicated that you are obligated not to use the private keys, certificates or any other technical support provided by UANATACA in carrying out any transaction prohibited by applicable law.

The digital certification services (and electronic time-stamping 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 that require error-proof 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 directly cause death, physical damage or serious environmental damage.

5. Obligations of the verifiers

5.1. 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.

5.2. Timestamp 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 a timestamp 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 timestamp to be verified is based, since it is verified using this certificate chain.

- It is necessary to ensure that the identified certificate chain is the most suitable for the timestamp being verified, since a timestamp 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 a timestamp 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 the certificate subscriber, as some certificates may include usage limits that prevent trusting the timestamp being verified. Each certificate in the chain has 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 for electronic timestamping.

5.3. Trust in an unverified certificate

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

5.4. 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 electronic time-stamping or certification public services without prior written consent.

Additionally, the verifier agrees not to intentionally compromise the security of UANATACA's public electronic time-stamping or certification services.

The electronic time-stamping and digital certification services provided by UANATACA have not been designed, nor are they permitted for use or resale, as equipment for controlling hazardous situations or for uses requiring fail-safe operations, 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.

5.5. 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.

UANATACA will not be liable in any case for any loss of encrypted information that cannot be recovered.

6. UANATACA 's Obligations

6.1. Regarding the provision of digital certification

UANATACA undertakes to:

a) To issue, deliver, manage, suspend, revoke and renew certificates, in accordance with the instructions provided by the subscriber, 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 in advance of the expiration date of the certificates.

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.

6.2. Regarding the registration checks

UANATACA is obligated to issue certificates based on the data provided by the subscriber, and may therefore carry out any checks it deems appropriate.

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 domain.

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.

6.3. 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.

7. Limited warranties and warranty disclaimers

7.1. 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 repository, that the certificate has been issued to the subscriber and domain 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 certificate contains the information that a qualified electronic seal certificate must contain, in accordance with Annex III of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014, and

with the additional instructions for the creation of qualified time stamps in accordance with Article 42 of the same Regulation.

- That, in the event that the subscriber's private keys are generated, their confidentiality is maintained during the process.

- The Certification Entity's responsibility is subject to the limits established. In no case will UANATACA be liable for acts of God or force majeure.

7.2. 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.

8. Agreements and policies

8.1. Applicable agreements

The agreements applicable to this certificate are as follows:

- Certification services contract, which regulates the relationship between UANATACA and the company subscribing to the certificates.

- General terms of service incorporated in the certificate disclosure text or PDS.

- DPC, which regulates the issuance and use of certificates.

8.2. DPC

UANATACA's certification and time-stamping services are regulated technically and operationally by UANATACA's DPC, its subsequent updates, and supplementary documentation.

The DPC and the documentation of operations are periodically modified in the Registry and can be consulted on the Internet page: https://www. UANATACA .com .

8.3. 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 judicial, administrative 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.

8.4. 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 user consent.

Furthermore, it is 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.

8.5. Refund policy

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

8.6. Applicable law and competent jurisdiction

Relations with UANATACA will be governed by Spanish law on trust services in force at any given time, as well as by civil and commercial legislation where applicable.

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

In the event of a disagreement between the parties, they shall attempt to resolve it amicably beforehand. To this end, the parties must send a communication to UANATACA by any means that provides proof of delivery to the contact address indicated in the contact information section of this PDS.

If the parties cannot reach an agreement in this regard, either of them may submit the dispute to civil jurisdiction, subject to the Courts of the registered office of UANATACA.

8.7. Accreditations and quality seals

Without stipulation.

8.8. Link to the list of providers

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

8.9. 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 the "Obligations and Responsibilities", "Compliance Audit" and "Confidentiality" sections of UANATACA's DPC will remain in effect after the termination of service.

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

The parties notify each other of facts through a procedure by sending an email to the address info@uanataca.com