Disclosure text - PDS (PKI Disclosure Statement) of the Qualified Authority for Electronic Timestamping

uanataca
trust service provider

Documentary control

Safety classification	**Public**
Version:	**2**
Edition date	**11/11/2021**
File	**PDS - TSA_EN_v2.docx**
Code	**PSC-3.3-**

Formal state

Prepared by :	**Revieweb by**	**Approved by**
Name: Alejandro Grande Date: 11/11/2021	Name: Albert Borrás Date: 12/11/2021	Name: Gabriel García Date: 16/11/2021

Version control

Version	Parts change	Description change	Author change	Change date
1.0	Original	Document creation	DMP	23/06/2017
2	Full	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

Index

INDEX 4

DISCLOSURE TEXT APPLICABLE TO THE ELECTRONIC SEAL CERTIFICATE OF THE QUALIFIED AUTHORITY FOR ELECTRONIC TIMESTAMPING 6

1. CONTACT INFORMATION 7
   1.1. RESPONSIBLE ORGANISATION 7
   1.2. CONTACT 7
   1.3. REVOCATION PROCEEDINGS CONTACT 7

2. TYPE AND PURPOSE OF THE CERTIFICATE 9
   2.1. CERTIFICATION AUTHORITY ISSUER 9

3. LIMITS OF USE OF CERTIFICATES 11
   3.1. LIMITS OF USE TARGETED TO SIGNERS 11
   3.2. LIMITS OF USE TARGETED TO VERIFIERS 11

4. SUBSCRIBERS’ OBLIGATIONS 13
   4.1. KEY GENERATION 13
   4.2. CERTIFICATES REQUEST 13
   4.3. REPORTING OBLIGATIONS 13
   4.4. CUSTODY OBLIGATIONS 14
   4.5. OBLIGATIONS OF PROPER USE 14
   4.6. PROHIBITED ACTIVITIES 15

5. VERIFIERS OBLIGATIONS 16
   5.1. INFORMED DECISION 16
   5.2. ELECTRONIC TIMESTAMPING VERIFICATION REQUIREMENT 16
   5.3. TRUSTING A CERTIFICATED NOT VERIFIED 17
   5.4. PROPER USE AND PROHIBITED ACTIVITIES 17
   5.5. INDEMNITY CLAUSE 18

6. UANATACA OBLIGATIONS 19
   6.1. REGARDING THE SERVICE OF DIGITAL CERTIFICATION 19
   6.2. REGARDING THE REGISTRY CHECKS 19
   6.3. PERIODS OF RETENTION 20

7. LIMITED GUARANTEES AND GURANTEES REJECTION 21

7.1. UANATACA GUARANTEES BY THE DIGITAL CERTIFICATION SERVICES 21
7.2. GUARANTEE EXCLUSION 22

8. AGREEMENTS AND STATEMENTS 23

8.1. APPLICABLE AGREEMENTS 23
8.2. CERTIFICATION PRACTICE STATEMENTS (CPS) 23
8.3. INTIMACY POLICY 23
8.4. PRIVACY POLICY 24
8.5. REFUND POLICY 24
8.6. APPLICABLE LAW AND COMPETENT JURISDICTION 24
8.7. ACCREDITATIONS AND QUALITY SEALS 25
8.8. LINKING WITH THE LIST OF PROVIDERS 25
8.9. SEVERALITY, SURVIVAL, ENTIRE AGREEMENT AND NOTIFICATION CLAUSES 25

DISCLOSURE TEXT APPLICABLE TO THE ELECTRONIC SEAL CERTIFICATE OF THE QUALIFIED AUTHORITY FOR ELECTRONIC TIMESTAMPING

This document contains the essential information in connection with the certification service of the Certification Authority of UANATACA.

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

1. Contact information

1.1. Responsible organisation

The Certification Authority UANATACA, known as “UANATACA”, is the result of:

UANATACA, S.A.
CALLE RIERA DE CAN TODÀ, 24-26, 6º, 1ª
08024 BARCELONA (SPAIN)
PHONE NUMBER: +34 935 272 290

1.2. Contact

For inquiries, please contact:

UANATACA, S.A.
CALLE RIERA DE CAN TODÀ, 24-26, 6º, 1ª
08024 BARCELONA (SPAIN)
PHONE NUMBER: +34 935 272 290
EMAIL: INFO@UANATACA.COM

1.3. Revocation proceedings contact

For inquiries, please contact:

UANATACA, S.A.
CALLE RIERA DE CAN TODÀ, 24-26, 6º, 1ª
08024 BARCELONA (SPAIN)
PHONE NUMBER: +34 935 272 290

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 UANATACA hierarchy
0.4.0.194112.1.3	In accordance with the Regulation UE (QCP-l-qscd)

The certificates of Authority for the Qualified Electronic Timestamping are qualified certificates according to Article 38 and with the Annex III of the Regulation (UE) 910/2014 of the European Parliament and Board, 23rd July of 2014 and have complied with the identified technical standards with the reference ETSI EN 319 412-3, ETSI EN 319 421 y ETSI EN 319 422.

These certificates allow the signature of digital evidence for timestamping.

The information of uses in the certificate's profile indicates the following:

a) The 'key usage' field is activated and therefore it allow us to perform the following function:
   a. Content commitment, for electronic signature

b) The 'extKeyUsage' field is activated and therefore it allow us to perform the following functions:
   a. 'timeStamping' para realizar la función de sellado de tiempo electrónico.
   b. The 'Qualified Certificate Statements' field appears in the following statement:
   c. qCCompliance (0.4.0.1862.1.1), that informs the certificate is issued as qualified.

c) The 'User Notice' field describe the use of this certificate.

2.1. Certification Authority issuer

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

3. Limits of use of certificates

3.1. Limits of use targeted to signers

The certification for the qualified electronic timestamping service provided by UANATACA can only be used for authorised uses in the contract signed between UANATACA and the SUBSCTIBER, and which are reproduced later (section “subscriber’s obligations”).

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

The subscriber must comply any law or regulation that may affect his right of use of the cryptographic tools used.

The subscriber cannot take actions of inspection, alteration or reverse engineering of the electronic timestamping services of UANATACA, without previous express permission.

3.2. Limits of use targeted to verifiers

Certificates are used for its own function and established purpose, without being able to be used in other functions and other purposes.

Similarly, certificates can only be used in accordance with the applicable law, specially taking into account the existing import and export restrictions at all times.

Certificates cannot be used to sign requests of issuance, renovation, suspension or revocation of certificates, nor public key certificates of any type, or Certificate Revocation List (CRL).

Certificates have not been designed, cannot be assigned and its use or resale as control equipment for dangerous situations is not authorised nor for uses that require fail- safe actions, such as operations of nuclear installation, navigation systems, air communications, or weapons control systems, where a failure could lead directly to death, personal injury or severe environmental damage.

There must be taken into account the limits indicated in the various fields of the certificates profiles, visible in the web of UANATACA (https://www.uanataca.com).

The use of the digital certificates in operations that violate this Certification Practice Statement (CPS), the binding legal documents with each certificate, or the contracts with the Registration Authorities or their signers/subscribers, is considered to misuse the legal purposes, exempting therefore to UANATACA, according to the current legislation, of any liability for this misuse of the certificates made by the signer or any third party.

Likewise, any responsibility that could result from the use of the custody out of the limits and conditions of use included in this Certification Practice Statement, the binding legal documents with each certificate, or the contracts or agreements with the registration authorities or with their subscribers, and any other misuse thereof derived from this section or may be interpreted as such according to the law, will be attributable to the subscriber, signer or the responsible of it.

4. Subscribers' obligations

4.1. Key generation

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

4.2. Certificates request

The subscriber is obliged to request the qualified certificates in accordance with the procedure and, if necessary, the technical components supplied by UANATACA, in accordance with what it is established in the certification practice statement (CPS) and UANATACA's operations documentation.

4.3. Reporting 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 UANATACA 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.

4.4. Custody obligations

The subscriber binds to custody all the information generated in its activity as Registration Authority.

The signer binds to custody the personal identification code or any other technical support delivered to UANATACA, the private keys and, if necessary, UANATACA 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 UANATACA by the subscriber.

4.5. Obligations of proper use

The signer must use the certificate only for authorized uses in the CPS and in any other instruction, manual or procedure supplied to the subscriber.

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

The signer will not be able to adopt the inspection, alteration or decompiling measures of the digital certification services provided.

The signer will recognise that:

a) When using any certificate, and while the certificate has not expired or been suspended or has been revoked, the certificate will be accepted and will be operative.

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

c) In case the private key is compromised, its use is immediately suspended and proceeds according to this document.

4.6. Prohibited activities

The verifier agrees not to use any private keys, certificates or any other type that has been supplied by UANATACA, in performing a prohibited transaction by the applicable law of that transaction.

Digital certification services (including electronic timestamping) provided by UANATACA have not been designed and its use or resale as control equipment for dangerous situations is not authorized nor for uses that require fail-safe actions, such as the operation of nuclear installation, navigation systems, air communications, or weapons control systems, where a failure could lead directly to death, personal injury or severe environmental damage.

5. Verifiers obligations

5.1. Informed decision

UANATACA informs the verifier 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 verifier 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.

5.2. Electronic timestamping verification requirement

The check is normally performed automatically by the software verifier and, in any case, according to the CPS, with the following requirements:

- It is necessary to use the appropriate software for the verification of a timestamping with the algorithms and key lengths authorised in the certificate and/or perform any other cryptographic operations, and establish the certificate chain based on electronic signatures to verify, since the electronic signature is verified using this certificate chain.
- It is necessary to ensure that the identified certificates chain is the most suitable for the timestamping to verify, since a timestamping may be based on more than one certificate chain, and it's up to the verifier make sure of the most appropriate chain for verification.
- It is necessary to check the revocation status of the certificates chain with the information provided to UANATACA Registry (with CRLs, for example) to determine the validity of all certificates in the certificate chain, since a timestamping can only be

considered properly verified if each and every certificate in the chain are correct and are in force.

- It is necessary to ensure that all certificates in the chain authorize the private key use by the certificate subscriber and the signer, since there is the possibility that any of the certificates include use limits that prevent rely on the timestamping to verify. Each certificate in the chain has an indicator that refers to the conditions of applicable uses, to review by the verifiers.
- It is necessary to technically verify all certificates signature in the chain before relying on the certificate used for the electronic timestamping.

5.3. Trusting a certificated not verified

If the verifier trusts a certificate not verified, he will assume all risks from that action.

5.4. Proper use and prohibited activities

The verifier agrees not to use any certificates status information or any other type that has been supplied by UANATACA, in performing a prohibited transaction by the applicable law of that transaction.

The verifier agrees not to inspect, interfere or perform any reverse engineer of the technical implementation of public services for electronic timestamping or certification of UANATACA without prior written consent.

In addition, the verifier binds not to intentionally compromise the security of public services electronic timestamping or certification of UANATACA.

The electronic timestamping services and of digital certification provided by UANATACA have not been designed and its use or resale as control equipment for dangerous situations is not authorized nor for uses that require fail-safe actions, such as the operation of nuclear installation, navigation systems, air communications, or weapons control systems, where a failure could lead directly to death, personal injury or severe environmental damage.

5.5. Indemnity clause

The relying third party in the certificate agrees to indemnify UANATACA 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 third 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.

UANATACA will not take responsibility in any case for loss of encrypted data that cannot be recovered.

6. UANATACA obligations

6.1. Regarding the service of digital certification

UANATACA undertakes:

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 UANATACA 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 and the signer, 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.

6.2. Regarding the registry checks

UANATACA undertakes to issue certificates based on the data supplied by the subscriber, so can perform the checks it deems appropriate.

In case UANATACA detects errors in the data to be included in the certificates or justify these data, will be able to make the necessary changes before issuing the certificate or suspend the issuance process and manage with the subscriber the corresponding effect. In case UANATACA corrects the data without prior management of relevant incident with the subscriber, it must notify the data finally certified to the subscriber.

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

The foregoing obligations shall be suspended in cases where the subscriber is acting as Registration Authority and has the technical elements corresponding to the key generation, certificate issuance and recording devices of corporate signature.

6.3. Periods of retention

UANATACA holds the corresponding issuance and revocation certificates requests logs for at least 15 years.

UANATACA holds the logs information for a period of between 1 to 15 years, depending on the type of information recorded, according to its policies and procedures.

7. Limited guarantees and gurantees rejection

7.1. UANATACA guarantees by the digital certification services

UANATACA guarantees to the subscriber:

- 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 Certification Practice Statement (CPS).

- That the revocation services and the use of the Deposit comply with all material requirements established in the Certification Practice Statement (CPS).

UANATACA guarantees the relying third party on the certificate:

- 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 Certification Practice Statement (CPS) has been accomplished.

- The rapidity and security in the certification services provision, especially in the revocation services and deposit.

In addition, UANATACA guarantees to the subscriber and the relying third party in the certificate:

- That the qualified certificate has the information that a qualified certificate for electronic timestamping must have, in accordance with Annex III of the Regulation (UE) 910/2014 of the European Parliament and Board, 23rd July of 2014 and with the additional indication for the creation of qualified timestamping in accordance with Article 42 of this Regulation.

- That, in case of private keys generated by the subscriber 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. UANATACA will not be responsible for fortuitous event or force majeure.

7.2. Guarantee exclusion

UANATACA rejects any other different guarantee to the previous that is not legally enforceable.

Specifically, UANATACA 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 UANATACA, except in cases where a written declaration to the contrary exists.

8. Agreements and statements

8.1. Applicable agreements

Applicable agreements to this certificate are the followings:

- Certification services contract, which regulates the relation between UANATACA and the subscribing certificates Company.
- Service general terms incorporated in this document
- CPS regulates the certificates issuance and use.

8.2. Certification practice statements (CPS)

UANATACA certification services and timestamping 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 is changed periodically in the Registry and can be consulted on the website: https://www.uanataca.com.

8.3. Intimacy policy

UANATACA cannot disclose or may be required to disclose any confidential information regarding certificates without prior specific request coming from:

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

b) Judicial, administrative or any other order provided in the current legislation.

However, the subscriber accepts that certain information, personal and any other type, provided in the certificate request, is included on the certificates and in the certificates status checking mechanism, and that the above information is not confidential, by legal imperative.

UANATACA does not give the data provided specifically for the certification services provision to anyone.

8.4. Privacy policy

UANATACA has a privacy policy under Section 9.4 of the CPS, and a specific regulation of the privacy related to the registration process, registration confidentiality, personal data protection, and the user consent.

Likewise, it is contemplated that the supporting documentation for the request approval must be preserved and properly registered with guarantees of security and integrity for a period of 15 years from the certificate expiration, even in case of early loss of effect for revocation.

8.5. Refund policy

UANATACA will not reimburse the cost of certification under any circumstance.

8.6. Applicable law and competent jurisdiction

UANATACA relations are governed by the Spanish law, as well as by civil and commercial legislation in all matters of application.

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

In case of disagreement between the parties, the parties will try an amicable settlement. For this purpose, the parties should address a communication to UANATACA, by any means, which they will leave a written record to the contact address indicated on this CPS.

In case the parties do not reach an agreement, any of them could refer the dispute to the civil jurisdiction, with subjection to Law Courts of the Registered Office of UANATACA.

8.7. Accreditations and quality seals

Not stipulated.

8.8. Linking with the list of providers

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

8.9. Severality, survival, entire agreement and notification clauses

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

The requirements contained in the sections of 'Obligations and responsibilities', of 'audit of conformity' and '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 info@uanataca.com.