Policy and Practice Statement of the Qualified Time Stamping Services

Trust Services

Evicertia
May 2021

1 Table of Contents

2 Introduction

2.1 Presentation

Evicertia, S.L. (Evicertia) is a Certification Service Provider (hereinafter referred to as “CPS”) that offers “Qualified Time Stamping Services” (QTSS) in accordance with Section 7 of REGULATION (EU) No. 910/2014 of the European Parliament and of the Council of July 23, 2014 2014 on electronic identification and trust services for electronic transactions in the internal market and for which it is repealed Directive 1999/93/EC.

2.2 Document Name and Identification

This document is the "Policy and Practice Statement of Qualified Time Stamping Services", hereinafter "PPSQTSS".

This document must be read along with Evicertia Trusted Services CPS, to which it is subordinated. Throughout this PPSQTSS, reference is made to sections of said CPS that will serve to complete this document.

2.3 Participants in the certification services

Review this section in Evicertia's CPS.

2.4 Use of time stamping service

2.4.1 Permitted uses

The Time Stamping service issues timestamps in order to prove that a series of data have existed and have not been altered from a specific moment in time. Its use is limited to the applications and/or systems of the clients (natural or legal persons) who have contracted these services.

2.4.2 Limits and prohibitions of use

The Time Stamping Service will not be used for purposes other than those specified in this document. Likewise, the service shall only be used in accordance with the applicable regulations.

2.5 Policy management

2.5.1 Organization that manages the document

The details of the company are the following:

- Evicertia, S.L. (Evicertia)
- VAT#: ESB86021839

- Madrid Mercantile Registry Volume: 28127, Book: 0, Folio 11, Section 8, Sheet M-506734, Registration 1.

2.5.2 Contact details of the organization

The contact details of Evicertia, S.L., are the following:

- Web: https://www.evicertia.com
- Email address: info@evicertia.com
- Phone: +34914237080
- Fax: +34911410144
- Postal address: Lagasca 95. 28006 Madrid. SPAIN.

2.5.3 Document management procedures

The documentary and organizational system of Evicertia guarantees, through the existence and application of the corresponding procedures, the correct maintenance of this document and the related service specifications.

3 Versions control

Version	Date	Comments
1.0	20/09/2019	The first version of this document is approved.
1.1	29/11/2019	Minor adequacy changes to the preliminary audit report.
1.2	12/05/2021	● Change of the name of the document to "Statement of Qualified Time Stamping Service Practices and Policies". ● With the name change, all references from CPS to PPSQTSS in the document itself are changed. ● Subordination reference of this document to the Evicertia CPD is added in section 2.2. ● Minor formatting and date updates to the cover page. ● Several sections of the document are modified to indicate that the information they contain is in the Evicertia CPD (2.3, 4.4, 7, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 10, and 11). ● A small change is made in section 4.2 to indicate that there are two public keys of certificates. ● Information about the *id-etsi-tsts-EuQCompliance* extension is added to section "6.3 Response Format".

4 Publication and preservation

4.1 Repository

Evicertia safely guards for at least 15 years every time stamp that is generated. It also has a Repository, in which information regarding the issuing service of qualified electronic time stamps is published. The publication repository can be found at https://www.evicertia.com/.

This service is available 24 hours a day, 7 days a week and, in case of a failure in the system outside of Evicertia's control, it will make its best for the service to be available again according to the deadlines and established procedures regarding business continuity.

4.2 Publication of information of the certification services provider

Evicertia will publish the following information in its repository:

- The Time Stamping Certification Practices Statement.
- The disclosure statement regarding the service
- The publics keys of the electronic time stamp certificates.

4.3 Publication frequency

The information of the CSP, including the DPS, CPS and this PPSQTSS, is published as soon as it is available.

Changes in the PPSQTSS are governed by what is established in the management procedure of this document and in accordance with the applicable regulations.

4.4 Access control

Review this section in Evicertia's CPS.

5 Identification and authentication

5.1 Initial registration

5.1.1 Types of names

The electronic Certificates used in the service of issuing qualified electronic time stamps, hereinafter "TSU Certificate/s", contain a distinguished name (*DN*) according to the X.501 standard in the Subject field, including a component *Common Name (CN =)*.

TSU Certificates are issued by Uanataca, SA, hereinafter "UANATACA". They are electronic certificates in accordance with Article 38 and Annex III of Regulation (EU) 910/2014 of the European Parliament

and of the Council, of July 23, 2014 and comply with the provisions of the technical regulations identified with references ETSI EN 319 412-3, ETSI EN 319 421 and ETSI EN 319 422.

5.1.2 Meaning of the names

The names contained in the *SubjectName* and *SubjectAlternativeName* fields of the certificates are understandable in natural language, in accordance with the provisions of the previous section.

5.1.3 Use of anonymous names and pseudonyms

N/A

5.1.4 Interpretation of name formats

Evicertia meets the requirements of the X500 standard.

5.1.5 Uniqueness of the names

The distinctive names of the TSU certificates will be unique.

5.2 Initial identity validation

N/A

5.3 Identification and authentication of renewal requests

N/A

5.4 Identification and authentication of the revocation, suspension or reactivation request

N/A

6 Operational requirements

6.1 Time stamp issuance request

6.1.1 Legitimation to request the time stamping service

The requesting party or user of the time stamping service can use their own application or software through the protocol defined in RFC 3161 and in accordance with ETSI 319 422, connecting to a website, and credential based access control, client certificate over HTTPS or IP address restriction.

Once the request has been accepted and registered and the appropriate checks have been carried out, the timestamp will be generated and sent to the requesting party.

6.1.2 Registration procedure and responsibilities

Evicertia receives requests for the time-stamping service, made by individuals, entities, companies or organizations of public or private law.

Requests shall be made using HTTPS protocol and ASN1 format according to the RFC3161.

6.2 Request Format

Stamp requests must be in accordance with the syntax of the "RFC 3161 Time Stamp Protocol (TSP)" specification, following the format specified in section 2.4.1 Request Format. The supported algorithms will be SHA-256, SHA-384 and SHA-512.

The time stamping service URLs will be, depending on the service, one of the following, taking into account that requests can only be made by HTTPS.

- https://tsa.evicertia.com/evitsa/qe1

The format for sending requests will be by HTTP POST request. The content of the request will be in ASN.1 encoded in DER, and must contain the following headers:

- Content type: `application/timestamp-query`
- Content-length: `required`

6.3 Response Format

The format of the responses will be via HTTPS. The format of the response content will be in ASN.1, encoded in DER, and will contain the following header.

- Content type: `application/timestamp-reply`

The answer is according to RFC 3161 section 2.4.2, in particular the contents of the `TSTInfo` token will contain the following fields:

- TSA: <TSA certificate DN>
- Time stamp: <the date of the stamp>
- Policy OID: 0.4.0.2023.1.1
- Ordering: no
- Hash Algorithm: sha256 (the algorithm is specified by the request)
- Serial number: <certificate's serial number>
- Accuracy: 0x01 seconds, unspecified millis, unspecified micross
- Nonce: unspecified.
- Extensions: *qcStatements (esi4-qtstStatement-1 identified by id-etsi-tsts-EuQCompliance).*

During the process, Evicertia:

- Protects the confidentiality and integrity of the registration data provided to it.
- Uses reliable systems and products that are protected against any alteration and that guarantee the technical security and, where appropriate, cryptography of the certification processes that they support.
- Indicates the date and time when a time stamp was issued.

6.4 Delivery and acceptance of the certificate

The delivery and acceptance of the TSU Certificates follow the procedures and directions established in the UANATACA Certification Practices Statement and Disclosure Text, both available on the website: https://www.uanataca.com.

6.5 Use of the key pair and certificate

The TSU Certificate uses solely the service of qualified electronic time stamps issuing service.

6.6 Certificate Modification

N/A

6.7 Revocation, suspension or reactivation of certificates

The procedures for revocation, suspension and reactivation of TSU Certificates follow the processes and indications established in the UANATACA Certification Practices Statement and Disclosure Text, both available on the website: https://www.uanataca.com.

- The revocation of a certificate implies the loss of its definite validity, and is irreversible.
- The suspension (or temporary revocation) of a certificate implies the loss of its temporary validity, and is reversible.
- The reactivation of a certificate implies its transition from a suspended state to an active state.

6.7.1 Causes for revocation of certificates

Evicertia will proceed to revoke the TSU Certificates when any of the following causes concur:

1. Circumstances that affect the information contained in the certificate:
    a. Modification of any data contained in the certificate, after the corresponding issuance of the certificate that includes the modifications.
    b. Discovery that any data contained in the certificate is incorrect.
2. Circumstances that affect the security of the key or certificate:
    a. Compromise of the private key, of the infrastructure or systems of the certification service provider that issued the certificate, provided that it affects the reliability of the certificates issued after that incident.

b. Infringement, by Evicertia, of the requirements set forth in the certificate management procedures, established in this Time Stamping Certification Practices Statement.
c. Compromise or suspicion of compromise of the security of the key or the certificate issued.
d. Unauthorized access or use by a third party of the private key corresponding to the public key contained in the certificate.

3. Other circumstances:
    a. The termination of the Evicertia certification service.
    b. The use of the certificate that is continually harmful for Evicertia. In this case, a use is considered harmful based on the following criteria:
        i. The nature and number of complaints received.
        ii. The identity of the entities that present the complaints.
        iii. The relevant legislation in force at all times.
        iv. The response of the subscriber or the person identified in the certificate to the complaints received.

6.7.2 Causes of suspension of a certificate

TSU Certificates may be suspended if the compromise of a key is suspected, until it is confirmed. In this case, Evicertia has to make sure that the certificate is not suspended for longer than necessary to confirm its compromise.

6.7.3 Causes of reactivation of a certificate

TSU Certificates can be reactivated.

6.7.4 Who can request the revocation, suspension or reactivation

The revocation, suspension or reactivation will be solicited by Evicertia.

6.7.5 Revocation, suspension or reactivation request procedures

The Procedure for requesting the revocation, suspension and/ or reactivation of TSU certificates follows the procedures and directions established in the UANATACA Certification Practices and Informative Text Statement, both available on the website: https: // www.uanataca.com.

6.7.6 Time period for request and processing of revocation, suspension or reactivation

The time period of the request a processing of the revocation, suspension and/ or reactivation of the TSU certificates follow the procedures and directions established in the UANATACA Certification Practices Statement and Disclosure Text, both available in the Website: https://www.uanataca.com

6.7.7 Obligation to check information about certificate revocation or suspension

Third parties must check the status of qualified electronic time stamps they wish to rely on, and to do so they should check the status of the TSU Certificate. A method by which the status of TSU certificates can be verified is by consulting the most recent Certificate Revocation List issued by the UANATACA Certification Entity, responsible for issuing them.

The Certificate Revocation Lists or CRL are published on the UANATACA website, as well as on the following web addresses, indicated in the certificates:

- http://crl1.uanataca.com/public/pki/crl/CA2subordinada.crl
- http://crl2.uanataca.com/public/pki/crl/CA2subordinada.crl

The validity status of certificates can also be checked by means of the OCSP protocol.

- http://ocsp1.uanataca.com/public/pki/ocsp/
- http://ocsp2.uanataca.com/public/pki/ocsp/

6.7.8 Frequency of issuance of certificate revocation lists (CRLs)

UANATACA, the certification authority issuing TSU certificates, issues an CRL at least every 24 hours.

The CRL indicates the scheduled time of issuance of a new CRL, although a CRL may be issued before the deadline indicated in the previous CRL, to reflect revocation.

The CRL keeps necessarily the certificate revoked or suspended until its expiry.

6.7.9 Maximum period of publication of CRLs

The CRLs are published in https:/www.uatanaca.com and in the indicated websites, in a reasonable period of time immediately after their generation, which in case exceeds a few minutes.

6.7.10 Availability of online certificate status checking services

Alternatively, third parties reliant on qualified electronic time stamps may consult the UANATACA Certificate Repository, which is available 24 hours a day, 7 days a week on the website:

- https://www.uanataca.com/public/pki/crtlist

To check the last CRL issued in each CA, the following downloads are needed:

- Root Certification Authority (UANATACA ROOT 2016):
  - http://crl1.uanataca.com/public/pki/crl/arl_Evicertia.crl
  - http://crl2.uanataca.com/public/pki/crl/arl_Evicertia.crl
- Intermediate Certification Authority 2 (UANATACA CA2 2016):
  - http://crl1.uanataca.com/public/pki/crl/CA2subordinada.crl

- http://crl2.uanataca.com/public/pki/crl/CA2subordinada.crl

6.7.11 Obligation to check verification services of certificates status

It is mandatory to check the status of TSU Certificates before relying on qualified electronic time stamps.

6.7.12 Special requirements in case of compromise of the private key

The compromise of the private key of the Evicertia TSU Certificates is notified to all participants in the certification services, as far as possible, by the publication of this fact on the Evicertia website, as well as, if considered necessary, in other media, even on paper.

6.8 Subscription Termination

N/A

6.9 Deposit and recovery of keys

6.9.1 Policy and practices of deposit and recovery of keys

N/A

6.9.2 Policy and practices of encapsulation and recovery of session keys

N/A

7 Physical, management and operations security controls

Review this section in Evicertia's CPS.

8 Technical security controls

Evicertia uses reliable systems and products, protected against any alteration and that guarantee the technical and cryptographic security of the certification processes they support.

8.1 Generation and installation of the key pair

8.1.1 Key pair generation

The key pair of the TSU Certificate is generated by the UANATACA Trust Services Provider, in accordance with its Certification Practices Statement and its disclosure text, being available on the website: www.uanataca.com.

Likewise, the Evicertia key ceremony procedures have been followed, within the high security perimeter assigned to this task. The activities carried out during the key generation ceremony have been registered, dated and signed by all the individuals participating in it, with the presence of an Auditor. Such records are kept for audit and follow-up purposes for an appropriate period determined by Evicertia.

Devices with the *FIPS 140-2 level 3 and Common Criteria EAL4+* certifications are used to generate the TSU certificate key.

The keys are generated using the RSA public key algorithm, with a minimum length of 2048 bits.

Certificates of the Time Stamp Unit	2.048 bits	Up to 8 years

8.1.2 8.1.2Sending the public key to the certificate issuer

The method of sending the public key to the electronic trust service provider is *PKCS#10,* another equivalent cryptographic test or any other method approved by Evicertia.

8.1.3 Distribution of the public key of the certification service provider

The Evicertia keys are communicated to third parties relying on certificates, ensuring the integrity of the keys and authenticating its origin, through its publication in the Repository.

Users can access the Repository to obtain public keys, and additionally, in S/MIME applications, the data message may contain a chain of certificates, which are thus distributed to users.

The certificate of the Root and Subordinate Certification Authorities will be available to users on the Evicertia website.

8.1.4 Key lengths

The length of the TSU Certificate keys is 2048 bits.

8.1.5 Generation of public key parameters

The public key of the TSU certificates is encrypted in accordance with RFC 5280.

8.1.6 Quality check of public key parameters

- Module length = 4096 bits
- Algorithm of keys generation: rsagen1
- Summary Cryptographic Functions: SHA256.

8.1.7 Key generation in computer applications or in capital goods

All keys are generated in capital goods, according to what is indicated in the section “Generation of the key pair”.

8.2 Private key protection

Review this section in Evicertia's CPS.

8.3 IT security controls

Review this section in Evicertia's CPS.

8.4 Technical life cycle controls

Review this section in Evicertia's CPS.

8.5 Network security controls

Review this section in Evicertia's CPS.

8.6 Engineering controls of cryptographic modules

Review this section in Evicertia's CPS.

8.7 Sources of Time

Review this section in Evicertia's CPS.

In addition to what is indicated in Evicertia's CPD, the accuracy of the Qualified Time Stamp of Evicertia is of **1 second** regarding *UTC (Universal Time Coordinated)*.

9 TSU certificate profile

The TSU certificate profile for the provision of the time stamping service follows the procedures and directions established in the UANATACA Certification Practices Statement and Disclosure Text, both available on the website: www.uanataca.com.

9.1 Certificate Profile

TSU certificates comply with the X.509 standard version 3, RFC 3739 and the EN 319 422 regulation.

9.1.1 Version number

The certificates are X.509 Version 3.

9.1.2 Certificate extensions

The certificate extensions are detailed in the profile documents that can be accessed on the UANATACA website (https://www.uanataca.com).

Thus, it is possible to keep more stable versions of the Certification Practices Statement and separate them from frequent profile adjustments.

9.1.3 Object identifiers (OID) of the algorithms

The object identifier of the signing algorithm is:

- 1.2.840.113549.1.1.11 sha256WithRSAEncryption

The object identifier of the public key algorithm is:

- 1.2.840.113549.1.1.1 rsaEncryption

9.1.4 Names Format

The certificates must contain the information that is necessary for their use, as determined by the corresponding policy.

9.1.5 Names Restriction

The names contained in the certificates are restricted to X.500 “Distinguished Names”, which are unique and unambiguous.

9.1.6 Object identifier (OID) of certificate types

All certificates include a certificate policy identifier under which they have been issued.

9.2 Certificate revocation list profile

The procedure for revocation, suspension and / or reactivation of TSU certificates follows the proceedings and directions established in the UANATACA Certification Practices Statement and Disclosure Text, both available on the website: www.uanataca.com.

9.2.1 Version number

The CRL issued by UANATACA are of version 2.

9.2.2 OCSP profile

According to the IETF RFC 6960 standard.

10 Compliance audit

Review this section in Evicertia's CPS.

11 Legal and commercial requirements

Review this section in Evicertia's CPS.

12 Annex I - Acronyms

The acronyms used in this Certification Practices Statement are shown below.

- CA: Certification Authority
- CN: Common Name
- CP: Certificate Policy
- CPS: Certification Practice Statement.
- CRL: Certificate Revocation List.
- CSP: Electronic Certification Services Provider/ Trust Service Provide
- CSR: Certificate Signing Request.
- DES: Data Encryption Standard.
- DN: Distinguished Name.
- DPC: Data Processing Center
- DSA: Digital Signature Algorithm.
- ETSI: European Telecommunications Standards Institute
- FIPS: Federal Information Processing Standard Publication.
- ISO: International Organization for Standardization.
- LDAP: Lightweight Directory Access Protocol.
- NTP: Network Time Protocol
- OCSP: On-line Certificate Status Protocol. OID: Object Identifier.
- PA: Policy Authority.
- PDS: Practice Disclosure Statement.
- PIN: Personal Identification Number.
- PKCS: Public-Key Cryptography Standards
- PKI: Public Key Infrastructure.
- PPSQERDS: Policy and Practice Statement of Qualified Electronic Registered Delivery Services
- PPSQTSS: Policy and Practice Statement of Qualified Time Stamping Services
- QERDS: Qualified Electronic Registered Delivery Services)
- QSCD: Qualified Signature Creation Device.
- RA: Registry Authority
- RSA: Rivest-Shimar-Adleman. Type of encryption algorithm
- SHA: Secure Hash Algorithm. Algoritmo seguro de Hash
- SSL: Secure Sockets Layer
- TCP/IP: Transmission Control. Protocol/Internet Protocol

- TSA: Time Stamping Authority
- TSU: Time Stamping Unity