Time Stamping Certification Practices Statement

Trust Services

EVICERTIA
November 2019

PUBLIC

1. Table of Contents

2. 2.Introduction

2.1. Presentation

This document states the certification practices of the issuing service of qualified electronic time stamps made by Evidencias Certificadas, S.L., hereinafter EVICERTIA.

2.2. Document Name and Identification

This document is the "EVICERTIA Time Stamping Certification Practices Statement", hereinafter "CPS".

2.3. Participants in the certification services

2.3.1. Certification service provider

The Electronic Certification Services Provider, hereinafter "CSP" is the person, natural or legal, who provides one or more trust services. EVICERTIA is an electronic trust service provider, that works in accordance with the provisions of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, as well as the technical standards of the ETSI applicable to the issuance of qualified electronic time stamps, mainly EN 319 421, in order to facilitate compliance with legal requirements and international recognition of their services.

2.3.2. Time stamping authority

The Time Stamping Authority, hereinafter referred to as "TSA" is the trusted third party that provides the service of issuing qualified electronic time stamps. EVICERTIA is the Certification Services Provider that acts as the Time Stamping Authority for the issuance of qualified electronic time stamps.

2.3.3. Certification service subscribers

Subscribers are the end users of qualified electronic time stamps issued by EVICERTIA. The subscribers of the service can be:

- Companies, entities, corporations or organizations that request EVICERTIA (directly or through a third party) to use it in their business, corporate or environment.

- Natural persons who request the service for themselves.

The subscriber of the electronic trust service is, therefore, a client of the Certification Services Provider.

2.3.4. User Parties

The user parties are the persons and organizations that receive the qualified electronic time stamps.

Previously to relying on time stamps, user parties must verify them, as established in this Certification Practice Statement.

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) that 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:

- Evidencias Certificadas, 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 Evidencias Certificados, 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.

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 seen 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 public key of the electronic time stamp certificate.

4.3. Publication frequency

The information of the Certification Services Provider, including the disclosure statement and the Time Stamping Certification Practices Statement, is published as soon as it is available.

Changes in the Time Stamping Certification Practices Statement are governed by the provisions of the management procedure of this document and in accordance with the applicable regulations.

4.4. Access control

EVICERTIA does not limit reading access to the information established in the section "Publication of information of the certification services provider", but it establishes controls to prevent unauthorized persons from adding, modifying or deleting records of the Repository, to protect the integrity and authenticity of the information.

EVICERTIA employs reliable systems for the Repository, so that:

- Only authorized persons can make notes and modifications.
- The authenticity of the information can be checked.

- Any technical change that affects the safety requirements can be detected.

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 distinguished 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 sending 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: <absent>

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

7.1. Physical security controls

EVICERTIA has established physical and environmental security controls to protect the resources of the facilities where the systems are, the systems themselves and the equipment used for the operations for the provision of electronic trust services.

Specifically, the EVICERTIA security policy applicable to electronic trust services establishes requirements for the following:

- Physical access controls.
- Protection against natural disasters.
- Protection measures against fire.
- Failure of support systems (electronic energy, telecommunications, etc.)
- Collapse of the structure.
- Floods.
- Anti-theft protection.
- Unauthorized departure of equipment, information, media and applications related to components used for the services of the certification service provider.

These measures are applicable to the facilities from which the electronic trust services are provided, in their production and contingency environments, which are periodically audited in accordance with the applicable regulations and EVICERTIA's own policies for this purpose.

The facilities have preventive and corrective maintenance systems with assistance 24h-365 days a year with assistance within 24 hours of the notice.

7.2. Location and building of the facilities

Physical protection is achieved by creating clearly defined security perimeters around the services. The quality and solidity of the building materials of the facilities guarantee adequate levels of protection against intrusions by brute force. They are located in an area of low disaster risk and allows for quick access.

The room where cryptographic operations are carried out in the main Data Processing Center has redundancy in its infrastructure, as well as several alternative sources of electricity and refrigeration in case of emergency.

EVICERTIA has facilities that physically protect the provision of services of certificate requests approval and of revocation management from the compromise caused by unauthorized access to the data, as well as to their disclosure.

7.2.1. Physical access

EVICERTIA has three levels of physical security in the main DPC (Building Entrance where it is located, access to the DPC room and access to the Rack), which must be accessed from the lower levels to the upper levels.

Physical access to the EVICERTIA units where certification proceedings are carried out is limited and protected by a combination of physical and procedural measures. Thus:

- It is limited to expressly authorized staff, with identification at the time of access and registration of it.
- The access to the rooms is made with ID card readers and/or electronic locks, managed by a computer system that maintains an automatic log in and out.
- To access the room where the cryptographic proceedings are located, prior authorization from EVICERTIA is necessary from the *colocation* service administrators who have the key to open the room and the cage, but not the cabinets.

7.2.2. Electricity and air conditioning

The EVICERTIA main DPC facilities have power stabilizer equipment and an equipment power supply system duplicated with a generator set.

The rooms that house computer equipment have temperature control systems with air conditioning equipment.

7.2.3. Exposure to water

The facilities are located in an area of low flood risk. The rooms that house computer equipment have a moisture detection system

7.2.4. Fire prevention and protection

The facilities and assets of EVICERTIA's main DPC have automatic fire detection and extinguishing systems.

7.2.5. Media storage

Only authorized staff have access to storage media. The information classified as of highest level is stored in a safe deposit outside the premises of the main Data Processing Center.

7.2.6. Waste treatment

The removal of media, both paper and magnetic, are carried out through mechanisms that guarantee the impossibility of recovering the information.

In the case of magnetic media, they are discarded, in which case they are physically destroyed, or reused after a process of permanent erasing or formatting. In the case of paper documentation, they are destroyed by shredders or in wastebaskets arranged for the purpose of being subsequently destroyed, under control.

7.2.7. Off-site backup

EVICERTIA uses a secure external warehouse for the custody of documents, magnetic and electronic devices that are independent of the main Data Processing Center.

7.3. Procedures control

EVICERTIA guarantees that its systems are operated safely, for which it has established and implemented procedures for the functions that affect the provision of its services.

The staff at the service of EVICERTIA executes the administrative and management procedures in accordance with the security policy.

7.3.1. Positions of trust

EVICERTIA has identified, according to its security policy, the following positions or roles with the condition of trust:

- **Internal Auditor:** Responsible for providing assurance of compliance with operating procedures by those responsible. This is a person outside the Information Systems department. The tasks of Internal Auditor are incompatible in time with the tasks of Certification and incompatible with Systems. These duties will be subordinated to the operations management, reporting both to it and to the technical management.
- **Systems Administrator:** Responsible for the proper functioning of the hardware and software support of the certification platform.
- **Security Manager**: Responsible for coordinating, controlling and enforcing the security measures defined by the security policies of EVICERTIA. He must take care of the aspects related to information security: logic, physical, networks, organizational, etc.
- **Systems Operator:** Responsible, alongside the Systems Administrator, for the correct operation of the hardware and software support of the certification platform. The operator is responsible for the backup and maintenance procedures of the daily operations of the systems.

- **Custodian:** Responsible for guarding the cryptographic cards where the pre-shared key is stored under the security model n of m. This function is compatible with the rest of the functions of this DPC

People who perform the aforementioned roles are subject to specific investigation and control procedures. Additionally, EVICERTIA implements criteria in its policies for the segregation of duties, as a measure of prevention of fraudulent activities.

7.3.2. Identification and authentication for each role

The people assigned for each role are identified by the internal auditor who will make sure that each person executes the tasks for which they have been assigned.

Each person only controls the assets that are necessary for their role, which ascertains that no one has access to unallocated resources.

Access to resources is made depending on the asset through username/password, digital certificate, physical access card and/or keys.

7.3.3. Roles that require segregation of duties

Positions of trust are established under the principle of minimum privilege, ensuring a segregation of duties, so that the person that has a role does not have total or especially broad control of all certification tasks, which ensures due control and surveillance, limiting thus any type of fraudulent behavior internally.

The granting of the minimum privilege for positions of trust will be done taking into account the best execution of the activity and will be as limited as possible, considering the organizational structure of EVICERTIA at all times.

7.4. Staff control

7.4.1. History, qualifications, experience and authorization requirements

All the staff is qualified and has been properly instructed to perform the operations that have been assigned to them.

The staff in positions of trust has no personal interests that conflict with the execution of the commissioned task.

In general, EVICERTIA will withdraw an employee from their position of trust when it becomes aware of the existence of conflicts of interest and/or the commission of any criminal act that could affect the performance of their duties.

EVICERTIA will not assign to a trust or management site a person who is not suitable for the position, especially for a fault that affects their suitability for the position. For this reason, an investigation is previously carried out to the extent permitted by the applicable legislation, regarding the following aspects:

- Studies, including alleged degree.
- Previous work, up to five years, including professional references.
- Professional references.

7.4.2. History investigation procedures

Before hiring a person or before the person enters their position, EVICERTIA performs the following checks:

- Work references of the last years.
- Professional references.
- Studies, including alleged degree.

EVICERTIA obtains the unambiguous consent of the concerned party for such prior investigation, and processes and protects all their personal data in compliance with current regulations on the protection of personal data, established in the General European Regulation No. 2016/679 of Data Protection and in general any national regulation that is applicable.

All checks are carried out to the extent permitted by the applicable law. The reasons that may lead to rejecting the candidate for a position of trust are the following:

- Falsehoods in the job application, made by the candidate.
- Very negative or very unreliable professional references in relation to the candidate.

7.4.3. Training requirements

EVICERTIA trains staff in reliable and management positions, until they reach the necessary qualification, keeping records of such training.

The training programs are periodically reviewed, and are updated for their best and periodically improved.

The training includes, at least, the following content:

- Tasks that the person must carry out.
- Security policies and procedures of EVICERTIA. Use and operation of installed machinery and applications.
- Management and processing of incidents and security compromises.
- Business continuity and emergency procedures.
- Management and security procedure in relation to the processing of personal data.

7.4.4. Requirements and frequency of formative update.

EVICERTIA updates the training of staff according to our needs, and with sufficient frequency for them to perform their duties competently and satisfactorily, especially when substantial modifications are made to the certification tasks.

7.4.5. Sequence and frequency of job rotation

N/A

7.4.6. Sanctions for unauthorized actions

EVICERTIA has a sanctioning system, to investigate and ascertain the responsibilities derived from unauthorized actions, in accordance with applicable labor legislation.

Disciplinary actions include suspension, separation of duties and even the dismissal of the person responsible for the harmful action, in proportion to the seriousness of the unauthorized action.

7.4.7. Requirements for hiring professionals

The employees hired to carry out the tasks of trust sign previously the confidentiality clauses and operational requirements implemented by EVICERTIA. Any action that compromises the safety of the accepted processes may, once evaluated, give rise to the termination of the employment contract.

In the case that all or part of the certification services are operated by a third party, the controls and forecasts made in this section, or in other parts of the Certification Practices Statement, will be applied and carried out by the third party who performs the tasks of operation of the certification practices. However, the Trust Service Provider will be responsible in any case for the actual execution. These aspects have been specified in the legal instrument used to agree on the provision of certification services by a third party other than EVICERTIA.

7.4.8. Provision of documentation to staff

The certification services provider shall provide the documentation that is strictly necessary at each moment, in order to carry out his duties in a competent and satisfactory manner.

7.5. Security Audit Procedures

7.5.1. Types of recorded events

EVICERTIA produces and keeps records, at least, of the following events related to the security of the entity:

- Activation and shutdown of the system.

- Attempts to create, delete, set passwords or change privileges.
- Attempts to start and end session.
- Attempts of unauthorized access to the TSA system through the network.
- Attempts of unauthorized access to the file system.
- Physical access to the logs.
- Changes in the settings and maintenance of the system.
- Registration of the TSA applications.
- Activation and shutdown of the TSA application.
- Changes in the TSA details and/or its keys.
- Records of the destruction of the media that contained the keys, activation data.
- Events related to the cycle of life of the cryptographic module, such as reception, use or uninstalling of it.
- The key generation ceremony and the key management databases.
- Physical access records.
- Maintenance and changes of the system settings.
- Staff changes.
- Reports of compromises and discrepancies.
- Records of the destruction of material containing key information, activation data or personal information of the subscriber, in the case of individual certificates, or of the natural person identified in the certificate, in the case of organization certificates.
- Complete reports of attempts of physical intrusion in the infrastructures that support the service.
- Events related to the synchronization and recalibration of the clock.

Registry entries include the following items:

- Date and time of entry.
- Serial number or sequence of the entry, in automatic records.
- Identity of the entity that is in the record.
- Entry type.

7.5.2. Frequency of processing audit records

EVICERTIA checks its logs when there is a system alert motivated by the existence of an incident.

The processing of the audit records consists of a review of the records that includes the verification that they have not been tampered with, a brief inspection of all the log entries and a deeper investigation of any alert or irregularity in the records. Actions carried out after the audit review are documented.

EVICERTIA keeps a system that allows to guarantee:

- Enough space for the storage of logs.
- That log files are not rewritten.

- That the information saved includes at least: type of event, date and time, user who executes the event and result of the operation.
- Log files will be stored in structured files that can be incorporated into a database for later exploration.

7.5.3. Period of retention of audit records

EVICERTIA stores the log information for a period of between 1 and 15 years, depending on the type of information recorded.

7.5.4. Protection of audit records

The audit log files are protected by physical and logical controls of access readings, modifications, unauthorized deletions.

Access to the log files is reserved only to authorized persons. There is an internal procedure detailing the management procedures of the devices that contain audit log data.

7.5.5. Backup procedures

EVICERTIA has an adequate backup procedure so that, in case of loss or destruction of relevant files, the corresponding backup copies of the logs are available in a short period of time.

7.5.6. Location of the audit log accumulation system

The event audit information is collected internally and automatically by the operating system, network communications and time-stamping software, in addition to the manually generated data, which will be stored by duly authorized staff. All this makes the system of accumulation of audit records.

7.5.7. Notification of the audit event to the causer of the event

When the audit log accumulation system records an event, it is not necessary to send a notification to the individual, organization, device or application that caused the event.

7.5.8. Vulnerability scan

Vulnerability scan is covered by EVICERTIA audit procedures.

Vulnerability scans should be executed, reviewed and checked through an examination of these monitored events. These analyzes must be carried out periodically in accordance with the internal procedure established for this purpose.

The audit data of the systems are stored in order to be used in the investigation of any incident and to locate vulnerabilities.

7.6. Information files

7.6.1. Record retention period

EVICERTIA archives the files specified above for at least 15 years, or the period established by current legislation.

The information files will be available for inspection by a qualified auditor based on compliance with current legislation.

7.6.2. File protection

EVICERTIA protects the file so that only duly authorized persons can access it. The file is protected against viewing, modification, deletion or any other manipulation, by being stored in a trusted system.

EVICERTIA ensures the correct protection of the files by assigning qualified staff for their processing and storage in secure external facilities.

7.6.3. Backup Procedures

EVICERTIA has a storage center outside of the main DPC to guarantee the availability of backup of the electronic file archive. Physical documents are stored in secure places with restricted access for authorized staff only.

EVICERTIA makes at least daily backup of all its electronic documents for data recovery cases.

7.6.4. Date and time stamp requirements

The records are dated with a reliable source via NTP. It is not necessary that this information is digitally signed.

7.6.5. Location of the file system

EVICERTIA has a centralized system of information gathering of the activity of the teams involved in the certificate management service.

7.6.6. Procedures for obtaining and verifying file information

EVICERTIA has a procedure that describes the process to verify that the filed information is correct and accessible. EVICERTIA provides the information and means of verification to the auditor.

7.7. Keys renovation

Each key pair of the TSU Certificates used in the time stamp service is only associated with the system that provides that service. Prior to the expiry of the use of the private key of the TSU Certificates, a change of keys will be made or revocation of the current ones.

7.8. Key compromise and disaster recovery

7.8.1. Procedures of incident and compromise management

EVICERTIA has developed security and business continuity policies that allow the management and recovery of the systems in case of incidents and compromise of its operations.

7.8.2. Corruption of resources, applications or data

When an event of corruption of resources, applications or data occurs, the appropriate management procedures will be followed in accordance with EVICERTIA's security and incident management policies, which include escalation, investigation and response to the incident. If necessary, EVICERTIA key compromise or disaster recovery procedures will be initiated.

7.8.3. Compromise of the private key of the entity

In the case of suspicion or knowledge of a compromise of EVICERTIA, the key compromise procedures will be activated, in accordance with the security policies, incident and business continuity management, that allows the recovery of the critical systems, if necessary in an alternative data center.

7.8.4. Business continuity after a disaster

EVICERTIA will restore critical services in accordance with the existing incidence and business continuity plan by restoring the normal operation of the previous services within 24 hours of the disaster.

7.9. Service termination

EVICERTIA ensures that possible interruptions to service subscribers and third parties will be minimal as a result of the cessation of the services of the certification service provider. In this sense, EVICERTIA guarantees a continuous maintenance of the defined records and for the time established in accordance with this Time Stamping Certification Practices Statement.

Notwithstanding the foregoing, if applicable, EVICERTIA will execute all the actions that are necessary to transfer to a third party or a notarial deposit the maintenance obligations of the records specified during the corresponding period according to this Time Stamping Certification Practices Statement or to the legal provision that corresponds.

Before finishing its services, EVICERTIA develops a termination plan, with the following provisions:

- It will provide the necessary funds, including civil liability insurance, to continue the completion of revocation activities.
- It will inform all Subscribers of the service, reliant Third Party and in general any third party with whom they have agreements or other type of termination relationship with a minimum anticipation of 2 months.
- It will transfer its obligations related to the maintenance of the information of the registry and of the logs during the period of time indicated to the subscribers and users.
- It will destroy or disable for use the private keys in charge of the time stamping service.
- It will perform the necessary tasks to transfer the maintenance obligations of the log information and the event log files during the respective time periods.
- It shall notify the corresponding Spanish Supervisory Body, at least 2 months in advance, of the cessation of its activity.
- Likewise, it will notify it of the opening of any bankruptcy process against EVICERTIA, as well as any other relevant circumstance that may prevent the continuation of the activity.

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. Sending 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

8.2.1. Cryptographic Module Standards

The modules that manage EVICERTIA keys comply with the *Common Criteria EAL4* + certification.

8.2.2. Private key control

The management of access to the private key of the TSU certificate is carried out according to the controls established by the HSM where they are kept. Also, cryptographic devices are physically protected as determined in this document.

8.2.3. Private key backup

EVICERTIA makes a backup copy of the private keys of the TSU certificates, so as to make their recovery possible in the event of a disaster, loss or deterioration thereof. Both the generation of the backup and its recovery need at least the participation of two people.

These recovery files are stored in fireproof cabinets and in the alternative custody center.

8.2.4. Entering the private key in the cryptographic module

Private keys are generated directly in the cryptographic production modules of EVICERTIA.

8.2.5. Private key activation method

The private keys of the TSU Certificates are stored encrypted in the cryptographic production modules of EVICERTIA.

8.2.6. Private key deactivation method

The EVICERTIA private key is activated by executing the corresponding secure start procedure of the cryptographic module.

8.2.7. Private key destruction method

To deactivate the EVICERTIA private key, the steps described in the corresponding cryptographic equipment manager's manual will be followed.

8.2.8. Classification of cryptographic modules

Prior to the destruction of the keys, a revocation of the certificate of the public keys associated with them will be issued.

- Devices that have stored any part of EVICERTIA's private keys will be physically destroyed or restarted at a low level. For the restart, the steps described in the cryptographic equipment manager manual will be followed.
- Finally, backup copies will be securely destroyed.

8.3. IT security controls

EVICERTIA uses reliable systems to offer its certification services. EVICERTIA has carried out IT controls and audits in order to establish management of its appropriate IT assets with the level of security required in the management of electronic certification systems.

Regarding information security, EVICERTIA applies the controls of the certification scheme on information management systems ISO 27001.

The equipment used is initially configured with the appropriate safety profiles by EVICERTIA systems staff, in the following aspects:

- Security configuration of the operating system.
- Application security settings.
- Correct system dimensioning.
- User settings and permissions.
- Log event setting.
- Backup and recovery plan.
- Requirements of network traffic.

The aforementioned functionalities are carried out by means of a combination of operating system, PKI software, physical protection and procedures.

8.4. Technical life cycle controls

8.4.1. System Development Controls

Applications are developed and implemented by EVICERTIA in accordance with development standards and change control.

The applications have methods for verifying integrity and authenticity, as well as correcting the version to be used.

8.4.2. Security management controls

EVICERTIA develops precise activities for the training and awareness raising of employees in matters of safety. The materials used for the training and the descriptive documents of the procedures are updated after their approval by a group for safety management. In carrying out this function, it has an annual training plan.

EVICERTIA requires security measures equivalent to any external provider involved in the work of electronic trust services.

8.4.2.1. Classification and management of information and goods

EVICERTIA keeps an inventory of assets and documentation and a procedure for the management of this material to guarantee its use.

The security policy of EVICERTIA details the information management procedures, where it is classified according to its level of confidentiality

The documents are catalogued on three levels: UNCLASSIFIED, INTERNAL AND CONFIDENTIAL USE.

8.4.2.2. Management operations

EVICERTIA has an adequate procedure for managing and responding to incidents, through the implementation of an alert system and the generation of periodic reports.

The incident management process is described in detail in the EVICERTIA security document.

EVICERTIA has documented the entire procedure related to the functions and responsibilities of the staff involved in the control and manipulation of elements contained in the certification process.

8.4.2.3. Media processing and safety

All media are processed safely in accordance with the requirements of the information classification. Media containing sensitive data are safely destroyed if they will not be required again.

8.4.2.4. System planning

The Systems Department of EVICERTIA keeps a record of the capabilities of the equipment. Together with the resource control application of each system, a possible redimensioning can be foreseen.

8.4.2.5. Reports of incidents and response

EVICERTIA has a procedure for the tracking of incidences and their resolution, where the responses and an evaluation of the resolution process of the incident are recorded.

8.4.2.6. Operational procedures and responsibilities

EVICERTIA defines activities, assigned to people with a role of trust, different from those in charge of carrying out daily operations that are not confidential.

8.4.2.7. Management of access to the system

EVICERTIA makes every effort that is reasonably within its reach to confirm that the access to the system is limited to authorized persons.

In particular:

- Firewall-based controls are available in high availability.
- Sensitive data is protected by cryptographic techniques or access controls with strong identification.
- EVICERTIA has a documented procedure for managing user registrations and deregistrations and access policy detailed in its security policy.
- EVICERTIA has procedures to ensure that operations are carried out in compliance with the role policy.
- EVICERTIA staff is responsible for their actions through the confidentiality agreement signed with the company.

8.4.2.8. Lifecycle management of cryptographic hardware

- EVICERTIA ensures that the cryptographic hardware used for the time stamping service is not handled during transportation by inspecting the delivered material.
- The cryptographic hardware moves on prepared media to avoid any manipulation.
- EVICERTIA records all relevant device information to add to the asset catalogue.
- The use of cryptographic time-stamping hardware requires at least two employees of trust.
- EVICERTIA performs periodic test tests to ensure the correct functioning of the device.
- The cryptographic hardware device is only handled by trusted staff.

- The private key of the EVICERTIA TSU certificate stored in the cryptographic hardware will be deleted once the device has been removed.
- The settings of the EVICERTIA system, as well as its modifications and updates are documented and controlled.
- Changes or updates are authorized by the security officer and are duly registered in the corresponding work records. These settings will be made by at least two trusted people.

8.5. Network security controls

EVICERTIA protects physical access to network management devices, and has an architecture that orders the generated traffic based on its security features, creating clearly defined network sections. This division is done through the use of firewalls.

Transference of confidential information over unsecured networks is done through encryption using TLS protocols or the VPN system with double factor authentication.

8.6. Engineering controls of cryptographic modules

Cryptographic modules are subject to the engineering controls provided for in the standards indicated throughout this section.

The key generation algorithms used are commonly accepted for the use of the key to which they are intended.

All cryptographic operations of EVICERTIA are carried out in modules with the *Common Criterial 4 EAL+* certification.

8.7. Sources of Time

The service of Qualified Time Stamping of EVICERTIA is based on the use of the *TSP protocol (TimepStamp Protocol)* over HTTP, defined in *RFC 3161 "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)"*.

All the devices used by EVICERTIA are synchronized by means of *NTP protocol (Network Time Protocol)* through internet (RFC 1305 Network Time Protocol), using one of the following stratum 1 NTP servers: *ntp.roa.es* or *hora.rediris.es*.

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

EVICERTIA has communicated the beginning of its activity as a provider of certification services by the National Supervisory Body, currently the Ministry of Industry, Commerce and Tourism, and is subject to the control reviews that this body deems necessary

10.1. Frequency of compliance audit

EVICERTIA carries out a compliance audit annually, in addition to the internal audits that it performs at its own discretion or at any time, due to a suspected breach of any security measure.

10.2. Auditor identification and qualification

The audits are performed by an independent external audit firm that demonstrates technical competence and experience in computer security, information systems security and compliance audits of public key certification services, and related elements.

10.3. Auditor's relationship with the audited entity

The auditing companies are of recognized prestige with departments specialized in the realization of computer audits, so there is no conflict of interest that could undermine its performance with regard to EVICERTIA.

10.4. List of elements subject to audit

The audit verifies regarding EVICERTIA:

1. That the entity has a management system that guarantees the quality of the service provided.
2. That the entity fulfils the requirements of the Certification Practices Statement and of other documentation related to the issuance of distinguished digital certificates.
3. That the Certification Practices Statement and other legal documentation are adjusted to the agreed by EVICERTIA and to the established in the current regulations.
4. That the entity manages adequately its information systems.

10.5. Actions to be taken as a result of a lack of conformity

Once the report of the compliance audit has been received by the management, the deficiencies found are analyzed with the company that has carried out the audit and the corrective measures that solve these deficiencies are developed and executed.

If EVICERTIA is unable to develop and / or execute the corrective measures or if the deficiencies found pose an immediate threat to the security or integrity of the system, it must immediately notify the EVICERTIA Management Board, that may execute the following actions:

- Cease operations temporarily.
- Revoke the TSU Certificate key and regenerate the infrastructure.
- Terminate the service of the Time Stamping Authority.
- Other complementary actions that are necessary.

10.6. Processing of audit reports

The audit results reports are delivered to the EVICERTIA Security Committee within a maximum period of 15 days after the execution of the audit.

11. Legal and commercial requirements

11.1. Fees

11.1.1. Time stamp service fee

EVICERTIA may establish a fee for the time-stamping service, of which, where appropriate, the subscribers will be informed in due course.

11.1.2. Access fee to time stamps status information

EVICERTIA has not established any fee for the access to time stamps status information.

11.1.3. Fees for other services

No stipulation.

11.1.4. Refund policy

No stipulation.

11.2. Financial capability

EVICERTIA has sufficient financial means to keep its operations and fulfil its obligations, as well as to face the risk of liability for damages, as established in ETSI EN 319 401-1 7.12 c), in relation to the management of the termination of services and cessation plan.

11.2.1. Insurance coverage

EVICERTIA has a guarantee of coverage of its sufficient civil liability, through professional civil liability insurance, which it maintains in accordance with current applicable regulations.

11.2.2. Other assets

No stipulation.

11.2.3. Insurance coverage for subscribers and third parties reliant on time stamps

EVICERTIA has a guarantee of sufficient civil liability coverage, through professional civil liability insurance, for electronic trust services, with a guaranteed minimum of 3,000,000 euros

11.3. Confidentiality

11.3.1. Confidential information

The following information is kept confidential by EVICERTIA:

- The service requests, as well as all other personal information obtained for the provision thereof, except for the information indicated in the following section.
- Transaction records, including complete records and transaction audit records.
- Internal and external audit records.
- Business continuity and emergency plans.
- Security plans.
- Documentation of operations, archiving, monitoring and other similar ones.
- All other information identified as "Confidential."

11.3.2. Legal Disclosure of Information

EVICERTIA will not disclose confidential information except in the cases provided for by law.

11.4. Personal data protection

EVICERTIA guarantees compliance with current regulations on the protection of personal data, established in the European Regulation 2016/679 General Data Protection and in general any national regulations that may apply.

In compliance with it, EVICERTIA has documented in this Certification Practices Statement of Time Stamping the security and organizational aspects and procedures, in order to ensure that all personal data to which it has access are protected against loss, destruction, damage, falsification and illegal or unauthorized processing.

Hereunder, all the necessary information regarding the processing of personal data carried out by EVICERTIA is detailed:

11.4.1. Data Controller

- Evidencias Certificadas, S.L. (EVICERTIA)
- NIF: ESB86021839

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

11.4.2. Contact details of the organization

- Data protection officer
- https://support.evicertia.com (main)
- Email: support+gdpr@evicertia.com
- Postal address: C/ Lagasca 95. 28006 Madrid, SPAIN.
- Telephone number: 914237080
- Fax number: 911410144

11.4.3. Purpose of the processing

EVICERTIA has a duty to inform users that all their personal data provided is processed for the following purposes:

- **Provision of Electronic Trust Services.** The data are collected through the appropriate contract and are processed in order to carry out the electronic services requested and contracted by the users, everything based on the established in this Time Stamping Certification Practices Statement.
- **Support for the provision of the Services.** Maintenance of contact details to facilitate the management of requests and incidents related to the provision of the Services. For example, the CLIENT or directly the User, can provide their contact details, to try to resolve an incident related to problems in the services offered by EVICERTIA.
- **Commercial Relationship.** Maintenance of contact details of CLIENT employees to facilitate the commercial management, billing, monitoring and management of the Services.

EVICERTIA informs that the personal data provided will only be processed for the purposes described above and will not be processed in a manner incompatible with them.

11.4.4. Legitimacy of the processing

According to the stated purposes of treatment, the legal basis for the processing of personal data of users is:

- The legitimacy of the processing for the Provision of Electronic Trust Services is the execution of the contract for the requested services, being the user a party in it.
- The legitimacy of the processing to attend the queries and requests is based on the consent of the interested party, which provides it expressly and unequivocally, through positive action before the sending, by accepting the conditions and the privacy policy.
- Such consent can be withdrawn at any time submitting a request at https://support.evicertia.com or by email at the contact email address.

11.4.5. Processed data and maintenance

The categories of personal data processed by EVICERTIA, include but are not limited to identifying data (name, surname and identity) and contact information (postal address, email and telephone number), and some additional information such as the IP address.

Personal data will be kept as long as they are necessary to respond to inquiries and requests, until the end of the contractual relationship and subsequently, during the legally required deadlines according to each case, as defined in this Certification Practices Statement.

11.4.6. Data transfer

Personal data will not be transferred to third parties except for legal obligation. Nor will international transfers be made.

11.4.7. Users Rights

- Confirmation. All users have the right to obtain confirmation about whether EVICERTIA is processing personal data that concerns them.
- Access and rectification. The uses have to right to access all their personal data, as well as to request the rectification of those that are inaccurate or erroneous.
- Deletion / cancellation. Users may request the deletion / cancellation of the data when, among other reasons, they are not necessary for the purposes for which they were collected.
- Limitation and opposition. The user may request the limitation of the processing so that their personal data are not applicable in some operations. In certain circumstances and for the reasons related to their particular situation, the user can oppose to the processing of data, being EVICERTIA bound to refrain from processing them, except for compelling legitimate reasons, or the exercise or defense of possible claims.
- Portability. The interested parties may request for their personal data to be sent to them or transmitted to another person in charge, in a structured electronic format and of regular use.

To exercise their rights, users can send a request at http://support.evicertia.com or a written request by email or by postal letter to the address indicated at **Contact details of the organization**. In such request, they must attach a copy of their identity document and clearly indicate the right to be exercised.

11.5. Intellectual Property Rights

EVICERTIA has intellectual property rights over this Time Stamping Certification Practices Statement.

11.6. Obligations and civil liability

11.6.1. Obligations of EVICERTIA

EVICERTIA guarantees, under its full responsibility, that it complies with all the requirements established in the Time Stamping Certification Practices Statement, being responsible for compliance with the procedures described, in accordance with the indications contained in this document.

EVICERTIA provides electronic trust services in accordance with this Time Stamping Certification Practices Statement.

EVICERTIA informs the subscriber of the terms and conditions related to the provision of the time-stamping service, its price and its limitations of use, by means of a subscriber contract that incorporates by reference the disclosure statements (PDS) of the service.

The disclosure statement, also called PDS, complies with the contents of Annex A of ETSI EN 319 421, a document which can be transmitted by electronic means, using a means of communication that is durable over time, and in understandable language.

EVICERTIA links subscribers and third parties relying on the certificates, through such disclosure statement or PDS, in written and understandable language, with the following minimum content:

- Requirements to comply with the provisions of this document.
- Limits of use of the time stamps.
- Information on how to validate a time stamp, including the requirement to check its status, and the conditions under which it can be reasonably trusted, which is applicable when the subscriber acts as a third party reliant on the certificate.
- How the state liability of the Certification Services Provider is guaranteed.
- Applicable limitations of liability, including the uses for which the Certification Service Provider accepts or excludes its liability.
- Archiving period of audit records.
- Applicable procedures of dispute resolution.
- Applicable law and competent jurisdiction.

11.6.2. Obligations of third parties in support services to the CSP

The obligations of third parties in support of the services offered by the CSP must provide, in general, the following guarantees:

- Comply with and facilitate compliance with everything stipulated in this CPS and in the CSP certification policies.
- Services whose infrastructure is deployed in third parties must offer the same levels of security and reliability as if they were deployed in the CSP infrastructure.

- The third party must know and follow what is established in this CPS and in the certification policies, being mandatory as if it were the CSP itself.
- In the case in which the third party also has to file information and data, it will do so under the same conditions and deadlines set by the CPS and the certification policies.
- The third party must inform the CSP of any changes that will be carried out in the infrastructure or in the procedures in order to submit it for evaluation by the PSC. In any case, these changes must guarantee the provisions of this CPS and the certification policies.

11.6.3. Guarantees offered to subscribers and relying third parties

EVICERTIA, in the documentation that binds it to subscribers and relying third parties, establishes and rejects guarantees, and applicable limitations of liability.

EVICERTIA guarantees to the subscriber that the time stamps meet all the material requirements established in this Certification Practice Statement, as well as the reference standards.

EVICERTIA guarantees the third party reliant on the qualified electronic time stamp that the information contained or incorporated by reference in it is correct, except when otherwise indicated.

11.6.4. Rejection of other guarantees

EVICERTIA rejects any other guarantee that is not legally enforceable, except those contemplated in this document.

11.6.5. Limits of liability

EVICERTIA limits its liability to the provision of the service of issuing qualified electronic time stamps which will be regulated by the appropriate contract.

EVICERTIA does not carry out any verification of the document for which the Time Stamp is requested, since it is sent directly by the Subscriber under his own and exclusive responsibility.

EVICERTIA assumes no obligation with respect to the monitoring of the content, type and/or format of the documents and the hash sent by the time-stamping process.

EVICERTIA will not be liable for any direct damage and/or by third parties as a result of improper use of qualified time stamps duly issued in accordance with this document.

11.6.6. Unforeseeable circumstances and force majeure

EVICERTIA includes in the disclosure statement or PDS, clauses that limit its liability in unforeseeable circumstances and in cases of *force majeure.*

11.6.7. Applicable Jurisdiction

EVICERTIA establishes, in the contract with the subscriber and in the disclosure statement or PDS, that the law applicable to the provision of services, including the certification policy and practices, is Spanish Law.

11.6.8. Severability, survival, entire agreement and notification clauses

EVICERTIA establishes, in the subscriber contract, and in the disclosure statement or PDS, severability, survival, entire agreement and notification clauses:

- Under the severability clause, the invalidity of a clause will not affect the rest of the contract.
- Under the survival clause, certain rules will continue in force after the termination of the legal relationship regulating the service between the parties. For this purpose, the Certification Entity ensures that, at least the requirements contained in the **Obligations and Liability**, **Compliance Audit** and **Confidentiality** sections, continue in force after the termination of the service and the general conditions of emission/use.
- Under the entire agreement clause, it will be understood that the legal regulatory document of the service contains the complete intent and all agreements between the parties.
- Under the notification clause, the procedure by which the parties notify each other will be established.

11.6.9. Competent jurisdiction clause

EVICERTIA establishes, in the subscriber contract and in the disclosure statement or PDS, a competent jurisdiction clause, indicating that the international judicial competence corresponds to the Spanish judges.

The territorial and functional competence will be determined by virtue of the rules of private international law and rules of procedural law that are applicable.

11.6.10. Conflict resolution

EVICERTIA establishes, in the subscriber contract, and in the disclosure statement or PDS, the applicable mediation and dispute resolution procedures.

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 Provider
- 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: Online Certificate Status Protocol
- OID: Object Identifier
- PA: Policy Authority
- PDS: Product Disclosure Statement
- PIN: Personal Identification Number
- PKCS: Public-Key Cryptography Standards
- PKI: Public Key Infrastructure
- QSCD: Qualified Signature Creation Device
- RA: Registry Authority
- RSA: Rivest-Shimar-Adleman. Type of encryption algorithm
- SHA: Secure Hash Algorithm
- SSL: Secure Sockets Layer
- TCP/IP: Transmission Control Protocol/Internet Protocol
- TSA: Time Stamping Authority
- TSP: Trust Service Provider
- TSU: Time Stamping Unity