

# Certification practice statement for timestamping service





# Certification practice statement for timestamping service

Público

## General Information

### Documental Control

|                                |                 |
|--------------------------------|-----------------|
| <b>Security Classification</b> | Public          |
| <b>Version</b>                 | 3.1             |
| <b>Edition Date</b>            | 20/07/2026      |
| <b>File</b>                    | DPC_TSA_EN_v3.1 |

### Formal State

|                                |                            |                                |
|--------------------------------|----------------------------|--------------------------------|
| <b>Prepared by</b>             | <b>Reviewed by</b>         | <b>Approved by</b>             |
| Raquel Fernández<br>20/07/2026 | Iria Baranda<br>20/07/2026 | Isidoro Martínez<br>20/07/2026 |

### Version control

| Version | What changes | Change description                                                                                      | Author           | Date       |
|---------|--------------|---------------------------------------------------------------------------------------------------------|------------------|------------|
| 1.0     | Original     | Document creation                                                                                       | Alejandro Grande | 23/03/2022 |
| 1.0     | No changes   | Annual revision                                                                                         | Leticia Faria    | 06/06/2023 |
| 1.0     | No changes   | Annual revision                                                                                         | Iria Baranda     | 12/06/2024 |
| 1.0     | 1.3.5        | Uanataca security standard version update                                                               | Iria Baranda     | 22/07/2024 |
| 1.0     | No changes   | Annual revision                                                                                         | Iria Baranda     | 10/06/2025 |
| 2.0     | 1.3.1        | The hierarchy of the certificates used is added.                                                        | Raquel Fernández | 15/09/2025 |
|         | 1.3.3.1      | The obligations of the subscribers are included in accordance with the terms and conditions of the TSA. |                  |            |
|         | 1.3.5.1      | Obligations relating to the                                                                             |                  |            |



## Certification practice statement for timestamping service

Público

|     |                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                     |            |
|-----|---------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|------------|
|     |                                                                                                                     | <p>Infrastructure Service Provider are added.</p> <p>4.7.7 Information on how to verify the time stamp is included.</p> <p>6.1.6 Corrections are made to adjust the key length value according to the technical configuration.</p> <p>6.1.8 Inclusion of details regarding the hash algorithms used in the service.</p>                                                                                                                                                                                           |                     |            |
| 3.0 | <p>1.3.1</p> <p>4.7.11</p> <p>5.9</p> <p>6.1.1<br/>6.2.1</p> <p>6.1.1<br/>6.1.4<br/>6.1.6</p> <p>6.7</p> <p>6.8</p> | <p>The hierarchy used in the provision of the service has been modified.</p> <p>Incorporation of trust anchor validation via TSL.</p> <p>The specified notice period prior to service termination has been updated to align with regulatory requirements.</p> <p>Details regarding the cryptographic devices used have been added.</p> <p>Update of the key sizes used.</p> <p>Details regarding the specified time sources have been corrected.</p> <p>Information regarding the service has been corrected.</p> | Raquel<br>Fernández | 11/06/2026 |



# Certification practice statement for timestamping service

Público

|     |       |                                                  |                     |            |
|-----|-------|--------------------------------------------------|---------------------|------------|
| 3.1 |       | The headings have been updated.                  | Raquel<br>Fernández | 20/07/2026 |
|     | 1.3.6 | Obligations of external organizations.           |                     |            |
|     | 9.4   | The link to the TECALIS repository is specified. |                     |            |

## Indice

|                                                                  |          |
|------------------------------------------------------------------|----------|
| <b>General Information</b>                                       | <b>2</b> |
| Documental Control                                               | 2        |
| Formal State                                                     | 2        |
| Version control                                                  | 2        |
| <b>Índice</b>                                                    | <b>3</b> |
| <b>Certification practice statement for timestamping service</b> | <b>9</b> |
| 1. Introduction                                                  | 9        |
| 1.1 Presentation                                                 | 9        |
| 1.2 Document Name And Identification                             | 9        |
| 1.3 Participants in The Certification Services                   | 9        |
| 1.3.1 Certification Service Provider                             | 9        |
| 1.3.2 Time Stamping Authority                                    | 9        |
| 1.3.3 Subscriber of the certification service                    | 9        |
| 1.3.3.1 Obligations of the Subscribers                           | 10       |
| 1.3.4 Relying Parties                                            | 10       |
| 1.3.5 Service Provider of the Technological infrastructure       | 10       |
| 1.3.5.1. Obligations of the Infrastructure Service Provider      | 11       |
| 1.3.6 Obligations of external organizations                      | 11       |
| 1.4 Use Of Timestamping Service                                  | 11       |
| 1.4.1 Permitted Uses                                             | 11       |
| 1.4.2 Prohibited Uses                                            | 12       |
| 1.5 Policy Management                                            | 12       |
| 1.5.1 Organization that administers the document                 | 12       |
| 1.5.2 Contact Information of the Organization                    | 12       |
| 1.5.3 Document management procedures                             | 12       |



# Certification practice statement for timestamping service

Público

|                                                                                         |    |
|-----------------------------------------------------------------------------------------|----|
| 2. Publication and Preservation                                                         | 13 |
| 2.1 Time Stamp Preservation                                                             | 13 |
| 2.2 Publication of Information of the Certification Services Provider                   | 13 |
| 2.3 Frequency of Publication                                                            | 13 |
| 2.4 Access Control                                                                      | 13 |
| 3. Identification and Authentication                                                    | 14 |
| 3.1 Initial Registration                                                                | 14 |
| 3.1.1 Type of Names                                                                     | 14 |
| 3.1.2 Meaning of the Names                                                              | 14 |
| 3.1.3 Use of anonymous and pseudonymous                                                 | 14 |
| 3.1.4 Interpretation of name formats                                                    | 14 |
| 3.1.5 Uniqueness of names                                                               | 14 |
| 3.2 Initial Identity Validation                                                         | 14 |
| 3.3 Identification and Authentication of Renewal Requests                               | 14 |
| 3.4 Identification and Authentication of Revocation, Suspension or Reactivation Request | 15 |
| 4. Operational Requirements                                                             | 16 |
| 4.1 Requests for Time Stamp                                                             | 16 |
| 4.1.1 Legitimation to apply for the issuance                                            | 16 |
| 4.1.2 Registration Procedure and Responsibilities                                       | 16 |
| 4.2 Processing the Request                                                              | 16 |
| 4.3 Time Stamp Issue                                                                    | 16 |
| 4.4 Certificate Delivery and Acceptance                                                 | 17 |
| 4.5 Key Pair and Certificate Usage                                                      | 17 |
| 4.6 Certificate Modification                                                            | 17 |
| 4.7 Revocation, Suspension or Reactivation of certificates                              | 17 |
| 4.7.1 Causes of Certificate Revocation                                                  | 18 |
| 4.7.2 Reasons for suspension of certificates                                            | 18 |
| 4.7.3 Reason for reactivation of certificates                                           | 18 |
| 4.7.4 Who can request the revocation, suspension or reactivation                        | 18 |
| 4.7.5 Procedures for revocation, suspension or reactivation request                     | 18 |
| 4.7.6 Temporary period of revocation, suspension or reactivation application processing | 18 |
| 4.7.7 Obligation to consult certificate revocation or suspension information            | 19 |
| 4.7.8 Frequency of issuance of certificate revocation lists (CRLs)                      | 20 |
| 4.7.9 Maximum period of publication of CRLs                                             | 20 |
| 4.7.10 Availability of the service checking in line with the state of the certificates  | 20 |
| 4.7.11 Obligation to check the consultation certificate status service                  | 20 |
| 4.7.12 Special Requirements in case of compromise of the private key                    | 20 |
| 4.8 Completion of the Subscription                                                      | 20 |



# Certification practice statement for timestamping service

Público

|                                                                            |    |
|----------------------------------------------------------------------------|----|
| 4.9 Deposit and Recovery of Keys                                           | 20 |
| 4.9.1 Policies and practices of deposit and key recovery                   | 20 |
| 4.9.2 Policy and practices of encapsulation and recovery of key session    | 21 |
| 5. Physical Security Controls, Management and Operations                   | 22 |
| 5.1 Physical Security Controls                                             | 22 |
| 5.2 Location and Construction of Facilities                                | 22 |
| 5.2.1 Physical Access                                                      | 23 |
| 5.2.2 Electrical Power and Air Conditioning                                | 23 |
| 5.2.3 Exposure to water                                                    | 23 |
| 5.2.4 Fire prevention and protection                                       | 23 |
| 5.2.5 Backup Storage                                                       | 23 |
| 5.2.6 Waste Management                                                     | 26 |
| 5.2.7 Offline Backup                                                       | 26 |
| 5.3 Procedure Controls                                                     | 26 |
| 5.3.1 Trust Roles                                                          | 26 |
| 5.3.2 Identification and authentication for each role                      | 25 |
| 5.3.3 Roles requiring separation of task                                   | 25 |
| 5.4 Personnel Controls                                                     | 25 |
| 5.4.1 History, qualification, experience and authorization requirements    | 26 |
| 5.4.2 Procedures of history investigation                                  | 26 |
| 5.4.3 Training requirements                                                | 26 |
| 5.4.4 Retraining frequency and requirements                                | 26 |
| 5.4.5 Job rotation frequency and sequence                                  | 27 |
| 5.4.6 Sanctions and authorized action                                      | 27 |
| 5.4.7 Professional contracting requirements                                | 27 |
| 5.4.8 Documentation supplied to personnel                                  | 27 |
| 5.5 Security Audit Procedures                                              | 27 |
| 5.5.1 Types of recorded events                                             | 28 |
| 5.5.2 Frequency of processing Audit Logs                                   | 28 |
| 5.5.3 Period of retention of audit logs                                    | 29 |
| 5.5.4 Audit logs protection                                                | 29 |
| 5.5.5 Audit log backup procedures                                          | 29 |
| 5.5.6 Location of the audit logs storage system                            | 29 |
| 5.5.7 Notification of the audit event to the subject that caused the event | 29 |
| 5.5.8 Vulnerability analysis                                               | 29 |
| 5.6 Information Files                                                      | 30 |
| 5.6.1 Retention period for the files                                       | 30 |
| 5.6.2 Protection of the file                                               | 30 |
| 5.6.3 File Backup procedures                                               | 30 |
| 5.6.4 Requirements of timestamping                                         | 30 |



# Certification practice statement for timestamping service

Público

|                                                                      |    |
|----------------------------------------------------------------------|----|
| 5.6.5 Location of the file system                                    | 30 |
| 5.6.6 Procedures to obtain and verify file information               | 31 |
| 5.7 Key Renewal                                                      | 31 |
| 5.8 Compromised Key and Disaster Recovery                            | 31 |
| 5.8.1 Management procedures of incidents and compromise              | 31 |
| 5.8.2 Resources, applications or data corruption                     | 31 |
| 5.8.3 Compromised private key of the entity                          | 31 |
| 5.8.4 Business continuity capabilities after a disaster              | 31 |
| 5.9 Service Termination                                              | 31 |
| 6. Technical Security Controls                                       | 33 |
| 6.1 Generation and Installation of Their Pair Keys                   | 33 |
| 6.1.1 Generation of the key pair                                     | 33 |
| 6.1.2 Sending of the public key to the certificate issuer            |    |
| 6.1.3 Public key distribution of the certification services provider | 33 |
| 6.1.4 Key Sizes                                                      | 34 |
| 6.1.5 Generation of public key parameters                            | 34 |
| 6.1.6 Quality check of the public key parameters                     | 34 |
| 6.1.7 Key generation in IT applications or in equipment good         | 34 |
| 6.1.8. Hash Algorithms Used in the Service                           | 34 |
| 6.2 Private Key Protection                                           | 35 |
| 6.2.1 Cryptographic modules standards                                | 35 |
| 6.2.2 Private key multi-person (n of m) control                      | 35 |
| 6.2.3 Private key backup                                             | 35 |
| 6.2.4 Private key transfer into a cryptographic module               | 35 |
| 6.2.5 Method of activating the private key                           | 35 |
| 6.2.6 Method of deactivating the private key                         | 35 |
| 6.2.7 Cryptographic modules classification                           | 36 |
| 6.3 Computer Security Controls                                       | 36 |
| 6.4 Life Cycle Technical Controls                                    | 37 |
| 6.4.1 System development controls                                    | 37 |
| 6.4.2 Security management controls                                   | 37 |
| 6.5 Engineering controls of Cryptographic Modules                    | 39 |
| 6.6 Time Sources                                                     | 39 |
| 6.7 Electronic Qualified Time Stamp Time Accuracy                    | 39 |
| 6.8 Change of State of a Qualified Signature Creation Device         | 40 |
| 7. TSU Certificate Profile                                           | 41 |
| 7.1 Certificate Profile                                              | 41 |
| 7.1.1 Version Number                                                 | 41 |
| 7.1.2 Certificate extensions                                         | 41 |
| 7.1.3 Object Identifier (OID) of the algorithms                      | 41 |



# Certification practice statement for timestamping service

Público

|                                                                                     |    |
|-------------------------------------------------------------------------------------|----|
| 7.1.4 Names Format                                                                  | 42 |
| 7.1.5 Names Restriction                                                             | 42 |
| 7.1.6 Object Identifiers (OID) of certificates types                                | 42 |
| 7.2 Certificate Revocation List Profile                                             | 42 |
| 7.2.1 Version Number                                                                | 42 |
| 7.2.2 OCSP profile                                                                  | 42 |
| 8. Compliance Audit                                                                 | 43 |
| 8.1 Frequency of Compliance Audit                                                   | 43 |
| 8.2 Identification and Qualification of the Auditor                                 | 43 |
| 8.3 Auditor Relationship to Audited Entity                                          | 43 |
| 8.4 Topics Covered by Audit                                                         | 43 |
| 8.4 Actions taken as a result of Lack of Conformity                                 | 43 |
| 8.5 Treatment of Audit Reports                                                      | 44 |
| 9. Business and Legal Requirements                                                  | 45 |
| 9.1 Fees                                                                            | 45 |
| 9.1.1 Timestamping service fees                                                     | 45 |
| 9.1.2 Timestamping status information Access fees                                   | 45 |
| 9.1.3 Fees for other services                                                       | 45 |
| 9.1.4 Refund Policy                                                                 | 45 |
| 9.2 Financial Capacity                                                              | 45 |
| 9.2.1 Cobertura de seguro                                                           | 45 |
| 9.2.2 Other assets                                                                  | 45 |
| 9.2.3 Insurance Coverage for subscribers and relaying third parties in certificates | 45 |
| 9.3 Confidentiality                                                                 | 46 |
| 9.3.1 Confidential Information                                                      | 46 |
| 9.3.2 Legal disclosure of information                                               | 46 |
| 9.4 Personal Data Protection                                                        | 46 |
| 9.5 Intellectual Property Rights                                                    | 48 |
| 9.6 Obligations and Civil Liability                                                 | 48 |
| 9.6.1 TECALIS Obligations                                                           | 48 |
| 9.6.2 Guarantees offered to subscribers and relying third parties in certificates   | 49 |
| 9.6.3 Rejection of other guarantees                                                 | 50 |
| 9.6.4 Limitation of liability                                                       | 50 |
| 9.6.5 Fortuitous event and force majeure                                            | 50 |
| 9.6.6 Applicable Law                                                                | 50 |
| 9.6.7 Severability, survival, entire agreement and notification clauses             | 50 |
| 9.6.8 Competent Jurisdiction Clause                                                 | 51 |
| 9.6.9 Resolution of conflicts                                                       | 51 |
| 10. Annex I - Acronyms                                                              | 52 |





# **Certification practice statement for timestamping service**

Público

# Certification practice statement for timestamping service

## 1. Introduction

### 1.1 Presentation

This document declares the certification practices for the service of issuing qualified electronic time stamps of TECALIS SOFTWARE SL, hereinafter TECALIS, by making use of the public key infrastructure (PKI) of Uanataca, S.A.

### 1.2 Document Name And Identification

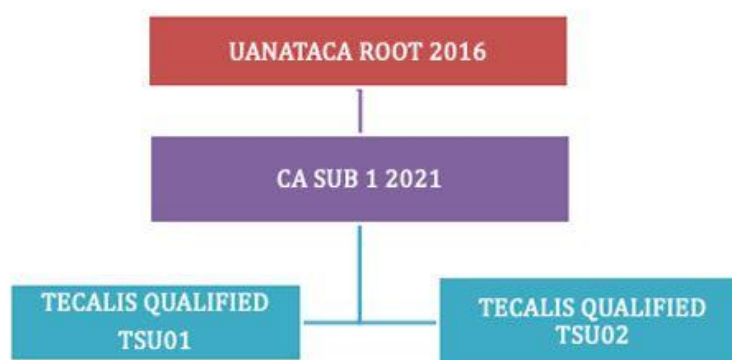
This document is the "TECALIS Time Stamping Certification Practices Statement".

### 1.3 Participants in The Certification Services

#### 1.3.1 Certification Service Provider

The electronic certification service provider (TSP / PSC) is the natural or legal person that provides one or more trust service. TECALIS is a trust service provider, acting in accordance with Regulation (EU) 910/2014 OF THE EUROPEAN PARLAMENT AND BOARD of 23rd July of 2014 related to the electronic identification and to the relying services for electronic transactions within the domestic market and repealing Directive 1999/93/CE, as well as the technical rules of the ETSI applicable to the issuance of qualified Time-Stamps, mainly the ETSI 319 421, in order to facilitate the legal requirements and international recognition of its services.

For the provision of the certification service, TECALIS has established a hierarchy of Certification Authorities:





## Certification practice statement for timestamping service Público

### 1.3.1.1. UANATACA ROOT 2016

This is the root Certification Authority of the hierarchy that issues certificates to certification authorities, and whose public key certificate has been self-signed.

Identification Data:

CN: UANATACA ROOT 2016

Thumbprint: 6d c0 84 50 a9 5c d3 26 62 c0 91 0f 8c 2d ce 23 0d 74 66 ad

Valid from: Friday, March 11, 2016

Valid until: Monday, March 11, 2041

RSA Key Length: 4,096 bits

### 1.3.1.2 CA SUB 1 2021

This is the Certification Authority within the hierarchy that issues certificates to end entities, and whose public key certificate has been digitally signed by UANATACA ROOT 2016.

Identification Data:

CN: UANATACA CA1 2021

Thumbprint: a1 db ea 6c 10 7a a3 e8 1e 16 c9 af 8e 55 7f ed 3d 90 cf 98

Valid from: Thursday, June 3, 2021

Valid until: Saturday, June 3, 2034

RSA Key Length: 4,096 bits

### 1.3.1.3 TECALIS QUALIFIED TSU 01

Identification Data:

CN: TECALIS QUALIFIED TSU 01

Thumbprint: a5 d5 d4 c3 f8 27 62 05 c3 60 6d ef a4 6d 8c 80 6f 46 a8 d2

Valid from: Friday, May 6, 2022

Valid until: Monday, May 6, 2030

RSA Key Length: 2,048 bits



## Certification practice statement for timestamping service Público

### 1.3.1.4 TECALIS QUALIFIED TSU 02

Identification Data:

CN: TECALIS QUALIFIED TSU 02

Thumbprint: 50 f2 63 cc 34 69 17 26 4c ba 8e 2d 68 92 c1 71 60 a9 c1 4d

Valid from: Wednesday, June 10, 2026

Valid until: Saturday, June 3, 2034

RSA Key Length: 3,072 bits

### 1.3.2 Time Stamping Authority

The Time Stamping Authority (TSA) is the trusted third party that provides the time stamping service. TECALIS is the trust service provider that provides the qualified time stamping service.

### 1.3.3 Subscriber of the certification service

The subscribers are the end users that receive the timestamps issued by TECALIS. The subscribers of the certification services are:

- Companies, entities, corporations and organizations that acquire them from TECALIS for its use in its business or organizational corporate level and which have been identified in the certificates.
- Natural persons that acquire the certificates for themselves and they have been identified in the certificates.

The subscriber of the trust service is the client of the Trust Service Provider.

#### 1.3.3.1 Obligations of the Subscribers

- Make requests for qualified electronic time stamps in accordance with the procedure and, if necessary, the technical components provided by TECALIS, in compliance with the provisions set forth in the Certification Practice Statement (CPS) and TECALIS documentation.
- Follow the instructions specified in TECALIS's TSU certificate PDS.
- Verify the electronic signatures of the electronic time stamps, including the validity of the certificate used.
- Use the electronic time stamps within the limits and scope described in this CPS and PDS.



## Certification practice statement for timestamping service Público

### 1.3.4 Relying Parties

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

To trust certificates, the relying parties must verify them, as it is established in the certification practice statement.

### 1.3.5 Service Provider of the Technological infrastructure

TECALIS and UANATACA, S.A. have signed a contract for the provision of technology services in which UANATACA will provide the public key infrastructure (PKI) that supports the trust service of TECALIS. UANATACA makes available to TECALIS the technical personnel necessary for the correct performance of the reliable functions of a Trusted Service Provider. UANATACA is the provider of Infrastructure services for certification services, provides its technological services to TECALIS so that it can carry out the services inherent to a Trusted Services Provider, always guaranteeing the continuity of services in the conditions and under the requirements demanded by the regulations.

UANATACA is a Trusted Service Provider accredited 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.

The PKI of UANATACA is subject to annual audits for the evaluation of the conformity of qualified providers of trust services according to the applicable regulations, under the norms:

- a) ISO/IEC 17065:2012
- b) ETSI EN 319 403
- c) ETSI EN 319 421
- d) ETSI EN 319 401
- e) ETSI EN 319 411-2
- f) ETSI EN 319 411-1

Also, UANATACA's PKI is subject to annual Audit under the security standards:

- a) ISO 9001:2015
- b) ISO/IEC 27001:2022

#### 1.3.5.1. Obligations of the Infrastructure Service Provider

The Public Key Infrastructure (PKI) service provider is obligated to make available to TECALIS the necessary technology services for the provision of certification services. In this regard:

- The provider shall have the necessary hardware to ensure that the aforementioned services are delivered with the security levels required by the applicable regulations.
  - It shall have the necessary software to ensure that the aforementioned services are delivered with the security levels required by the applicable regulations.
  - It shall guarantee the custody and hosting of the systems (hardware and software) in a Data Processing Center (Data Center) with appropriate logical and physical security levels, in accordance with generally accepted international standards.
  - It shall be responsible for carrying out all preventive, evolutionary, corrective, reactive, and,



## Certification practice statement for timestamping service

Público

in general, any other maintenance required by the technological infrastructure for the provision of technology services.

- It shall be responsible for providing third-level technical support, meaning it shall provide technical support for issues that exceed TECALIS's management capacity and are directly related to deficiencies and/or technical failures in the technological infrastructure.
- In providing services to TECALIS, the provider shall make available the necessary technical personnel for the operation of the public key infrastructure, who shall perform the trusted roles dedicated to the administration and operation of the systems, specifically:

- PKI Security Officer
- Internal Auditor
- System Administrator
- System Operator
- CA Administrator
- CA Operator

### 1.3.6 Obligations of external organizations

Any external organization participating in the provision of trust services undertakes to:

- Comply with the service levels, security, and confidentiality agreed upon contractually with TECALIS.
- Provide its services in accordance with the requirements established in this Certification Practice Statement and the applicable regulations (eIDAS Regulation and corresponding ETSI standards).
- Notify TECALIS, without undue delay, of any incident, vulnerability, or security compromise that may affect the provision of the trust service.
- Cooperate with TECALIS and, where applicable, with the conformity assessment body and the supervisory authority, within the framework of conformity audits and other applicable control processes.
- Ensure the protection of personal data processed in the context of the provision of its services, pursuant to applicable data protection regulations.

## 1.4 Use Of Timestamping Service

### 1.4.1 Permitted Uses

The Time Stamping service issues time stamps in order to prove that a data has existed and has not been altered from a specific moment in time. The use of the time stamping service is limited to the applications and / or systems of clients (individuals or legal entities) that have contracted these services.



## Certification practice statement for timestamping service

Público

The Time Stamping Services from TECALIS are identified with OID: 1.3.6.1.4.1.58758.2

### 1.4.2 Prohibited Uses

The Time Stamping Service will not be used for purposes other than those specified in this document. In the same way, the service should only be used in accordance with the applicable regulation.

## 1.5 Policy Management

### 1.5.1 Organization that administers the document

Tecalís Software S.L.

Rúa Oliveira 35, Parque empresarial Novo Milladoiro, 15895 Milladoiro-Ames

A Coruña, España

+34 911 01 07 00

[hello@tecalis.com](mailto:hello@tecalis.com)

### 1.5.2 Contact Information of the Organization

Tecalís Software S.L.

Rúa Oliveira 35, Parque empresarial Novo Milladoiro, 15895 Milladoiro-Ames

A Coruña, España

+34 911 01 07 00

[hello@tecalis.com](mailto:hello@tecalis.com)

### 1.5.3 Document management procedures

The documental and organization system of TECALIS guarantees, according to the existence and request of the corresponding procedures, the correct maintenance of this document and the specification of the service related to itself.



## Certification practice statement for timestamping service Público

## 2. Publication and Preservation

### 2.1 Time Stamp Preservation

TECALIS safely store all time stamps generated for at least 15 years. Likewise, it has a published deposit, where all the information related with the time stamping service is stored.

That service is available 24 hours, 7 days per week and, in case of the system failure was under TECALIS's control, it will make its best efforts to ensure that the service is back available according with established deadlines and procedures with respect the business continuity plan.

### 2.2 Publication of Information of the Certification Services Provider

TECALIS publishes the following information, in its Deposit:

- The Certification Practice Statement for time stamping service.
- Policy disclosure statements (PDS).
- The public key of the TSU certificate.
- References to the validation service of Time Stamps.

### 2.3 Frequency of Publication

The information of the certification services provides, including the policies and the Certification Practice Statement, is published when available.

The changes on the Certification Practice Statement shall be governed by the established in the change management procedure and in accordance with the applicable regulations.

### 2.4 Access Control

TECALIS does not limit the read access to the information established in the section 2.2 but establishes controls to prevent non-authorized people to add, modify or delete registrations of the Deposit, to protect the integrity and authenticity of the information.

TECALIS uses reliable systems for the Deposit, in such a way that:

- Only authorized persons could do annotations and modifications.
- The authenticity of the information could be verified.
- Any technical change affecting the security requirements could be detected.





## Certification practice statement for timestamping service Público

### 3. Identification and Authentication

#### 3.1 Initial Registration

##### 3.1.1 Type of Names

All the certificates used in the Time Stamping provision, hereinafter “TSU Certificate”, contain a distinguished name (DN) X.501 in the field Subject including a component Common Name (CN=).

The TSU Certificates are issued by Uanataca, S.A., hereinafter “UANATACA”, these certificates are issued according to the article 38 and the Annex III of the 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 and they are compliant with the technical regulations identified with the references ETSI EN 319 412-3, ETSI EN 319 421 y ETSI EN 319 422.

##### 3.1.2 Meaning of the Names

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

##### 3.1.3 Use of anonymous and pseudonymous

N/A

##### 3.1.4 Interpretation of name formats

TECALIS is compliant with the requirements of the X.500 standard.

##### 3.1.5 Uniqueness of names

The distinguished name of the TSU Certificates will be unique.

#### 3.2 Initial Identity Validation

N/A

#### 3.3 Identification and Authentication of Renewal Requests

N/A



## Certification practice statement for timestamping service

Público

### 3.4 Identification and Authentication of Revocation, Suspension or Reactivation Request

N/A



## Certification practice statement for timestamping service Público

### 4. Operational Requirements

#### 4.1 Requests for Time Stamp

##### 4.1.1 Legitimation to apply for the issuance

The requester or user of the Time Stamping service, a natural or legal person, can make a request of a qualified time stamp by a direct request to TECALIS or through the available TSA server, which allows the time stamping of the documents.

The requester or user of the Time Stamping service can use their own application or software through the protocol defined in RFC 1361 and in accordance with ETSI 319 422, all by connecting to a web address and using credentials provided by TECALIS.

Once the request has been accepted, registered and the appropriate verifications have been done, the timestamp is issued and sent to the requester.

##### 4.1.2 Registration Procedure and Responsibilities

TECALIS receives requests for the time stamping service, made by persons, entities, companies or organization of public or private law.

Applications are made directly through the TECALIS computer systems.

#### 4.2 Processing the Request

The requester submits through the established procedures, the application of the time stamp for an electronic document directly to the time stamping service / server in charge of the sealing. First the petition shall be made, after the document shall be send to the corresponding web direction, after the documents will be duly sealed and returned.

#### 4.3 Time Stamp Issue

The qualified time stamps are automatically issued through the system or server which is providing the time stamping service. After the approval of the time stamp request, the time stamp is issued securely and made available to the subscriber.

During the process, TECALIS:

- Protects the confidentiality and integrity of the registration data that owns.
- Uses reliable systems and products that are protected against every disturbance and guarantee the technical security and, in its case, cryptographic security of the processes of certification to which they support.



## Certification practice statement for timestamping service Público

- Indicates the date and hour in which a time stamp was issued

### 4.4 Certificate Delivery and Acceptance

The delivery and acceptance of the TSU Certificates follow the processes and indications established in the Certification Practice Statements and the PDS of UANATACA as Certification Authority, all available on the website: <https://web.uanataca.com/>.

### 4.5 Key Pair and Certificate Usage

The TSU Certificate is exclusively used for the service of issuing qualified electronic time stamps.

### 4.6 Certificate Modification

N/A

### 4.7 Revocation, Suspension or Reactivation of certificates

The revocation of a certificate means the definitive withdrawal of the certificate and it is irrevocable.

The suspension (or temporal revocation) of a certificate means the temporal withdrawal of it and it is reversible. Only end entity certificates will be able to be stopped.

The reactivation of a certificate is the transition from a hold status to an active state.

The procedures for revocation, suspension and reactivation of the TSU Certificates follow the processes and indications established in the Certification Practice Statements and the PDS of UANATACA, all available on the website: [www.uanataca.com](http://www.uanataca.com).

#### 4.7.1 Causes of Certificate Revocation

TECALIS will revoke the TSU Certificate when any of the following causes occur:

1. Circumstances affecting the information contained in the certificate:
  - a. Modification of any of the data contained in the certificate, after the corresponding issue of the certificate including amendments.
  - b. Discovery that any of the data contained in the certificate application is incorrect.
  - c. Discovery that any of the data contained in the certificate is incorrect
2. Circumstances affecting the security of the key or certificate:
  - a. Compromise of the private key, infrastructure or systems certification service provider that issued the certificate, provided that it affects the reliability of the certificates issued from that incident.
  - b. Infringement, by TECALIS, of the requirements of the certificate management procedures established in this Certification Practice Statement.



## Certification practice statement for timestamping service

Público

- c. Compromise or suspected compromise of the security key or certificate issued.
- d. Unauthorized access or use, by a third-party private key corresponding to the public key contained in the certificate.
- 3. Other circumstances:
  - a. Termination of Certification Service of TECALIS.
  - b. The use of the certificate that is harmful and continued to TECALIS. In this case, it is considered that a use is harmful in terms of the following criteria:
    - The nature and number of complaints received.
    - The identity of the entities filing complaints.
    - The relevant legislation in force at all times.
    - The response of the subscriber or of the person identified in the certificate to complaints received.

### 4.7.2 Reasons for suspension of certificates

TSU Certificates can be suspended if a key compromise is suspected, until it is confirmed. In this case, TECALIS must ensure that the certificate is not suspended for longer than necessary to confirm its compromise.

### 4.7.3 Reason for reactivation of certificates

The TSU Certificates can be reactivated.

### 4.7.4 Who can request the revocation, suspension or reactivation

The revocation, suspension or reactivation will be requested by TECALIS.

### 4.7.5 Procedures for revocation, suspension or reactivation request

The procedures for revocation, suspension or reactivation of the TSU Certificates follow the processes and indications established in the Certification Practice Statements and the PDS of UANATACA, all available on the website: [www.uanataca.com](http://www.uanataca.com)

### 4.7.6 Temporary period of revocation, suspension or reactivation application processing

The temporary period of revocation, suspension or reactivation application processing follow the processes and indications established in the Certification Practice Statements and the PDS of UANATACA, all available on the website: [www.uanataca.com](http://www.uanataca.com).



## Certification practice statement for timestamping service Público

### 4.7.7. Obligation to Check Revocation or Suspension Information of Certificates

Third parties must verify the status of the qualified electronic time stamps they wish to rely on; to do so, they must check the status of the TSU Certificate.

One method to verify the status of TSU certificates is by consulting the most recent Certificate Revocation List (CRL) issued by the TECALIS Certification Authority responsible for issuing them.

The Certificate Revocation Lists (CRLs) are published on the TECALIS website, as well as at the following web addresses, indicated within the certificates:

- Subordinate Certification Authority - UANATACA CA1 2021
  - <http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl>
  - <http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl>

The validity status of certificates can also be checked via the OCSP protocol:

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

Third parties must verify the status of the qualified electronic time stamps they wish to rely on; to do so, they must check the status of the TSU Certificate.

One method to verify the status of TSU certificates is by consulting the most recent Certificate Revocation List (CRL) issued by the TECALIS Certification Authority responsible for issuing them.

The Certificate Revocation Lists (CRLs) are published on the TECALIS website, as well as at the following web addresses, indicated within the certificates:



## Certification practice statement for timestamping service Público

### 4.7.8 Frequency of issuance of certificate revocation lists (CRLs)

UANATACA issues a CRL at least every 24 hours.

The CRL indicates the scheduled time of issuance of a new CRL, although it may issue an CRL before the deadline stated in the previous CRL, to reflect revocations.

The CRL is obliged to maintain the revoked or suspended certificate until it expires.

### 4.7.9 Maximum period of publication of CRLs

The CRLs are published in the Deposit within a reasonable period immediately after their generation, which in any case is no more than a few minutes.

### 4.7.10 Availability of the service checking in line with the state of the certificates

Alternatively, third parties who rely on the Time Stamps issued by TECALIS may consult UANATACA deposit certificates, which is available 24 hours 7 days a week on the web:

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

To check the latest CRL issued in the CA, the following may be downloaded:

Certification Authority (CA) Intermediate 1 - UANATACA CA1 2021

- <http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl>
- <http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl>

### 4.7.11 Obligation to check the consultation certificate status service

It is mandatory to check the status of the TSU certificates before relying on the Time stamps issued by TECALIS.

In addition to checking the revocation or suspension status of the certificate through the corresponding validation services (CRL and/or OCSP), for a TSU certificate to be used in the provision of a qualified electronic time-stamping service, relying parties must verify that the trust anchor used for the certificate validation is identified as a qualified trust service in a valid entry of the European Union Trust List.

### 4.7.12 Special Requirements in case of compromise of the private key

The compromise of the private key of TSU Certificate of TECALIS is notified to all participants in certification services, as far as possible, by posting this in the website and, if deemed necessary, in other media, even on paper.



## Certification practice statement for timestamping service

Público

### 4.8 Completion of the Subscription

N/A

### 4.9 Deposit and Recovery of Keys

#### 4.9.1 Policies and practices of deposit and key recovery

N/A

#### 4.9.2 Policy and practices of encapsulation and recovery of key session

N/A





## Certification practice statement for timestamping service Público

### 5. Physical Security Controls, Management and Operations

#### 5.1 Physical Security Controls

TECALIS provides the trust services through the public key infrastructure of UANATACA, which has established physical and environmental security controls to protect the resources of the facilities where the systems are located, the systems and the equipment used for the operations for the provision of trustworthy electronic services.

Specifically, the security policy applicable to the trust electronic services has established requirements for the following contingencies:

- Physical access controls.
- Protection against natural disasters.
- Protective measures against fires.
- Failure of the support systems (electronic energy, telecommunications, etc.)
- Collapse of the building.
- Flooding.
- Antitheft protection.
- Unauthorized removal of equipment, information, media and applications relating to components used for the services of the service provider certification.

These measures are applicable to installations where the trust services are provided, which lends from its both mainstream and, where appropriate, operating in contingency high security installations that are properly audited periodically.

Facilities include preventive and corrective maintenance systems with assistance 24/7 all year round with assistance in the following 24 hours notice.

#### 5.2 Location and Construction of Facilities

The facilities that make up the TECALIS Public Key Infrastructure are located in a rack / cabinet physically isolated from the rest of the infrastructure hosted at the Data Processing Centre of the technology service provider ADAM Ecotech (hereinafter ADAM), located in Barcelona, Spain.

Physical protection is achieved by creating clearly defined security perimeters around services. The quality and strength of building materials facility ensures adequate levels of protection against intrusion by brute force and located in an area of low risk of disasters and allows quick access.



## Certification practice statement for timestamping service Público

The room where the cryptographic operations are performed in the Data Processing Centre has redundancy in its infrastructure, as well as several alternative sources of power and cooling in an emergency.

Facilities are available to physically protect the provision of services approval of applications for certificates and revocation management, compromise caused by unauthorized access to systems or data access and disclosure thereof.

### 5.2.1 Physical Access

There are three levels of physical security (building entrance where the CPD is found, access to the room of the CPD and access to the rack) for service of protecting the certificate generation and must be accessed from the lower to the upper levels.

Physical access, where certification is processed, is limited and protected by a combination of physical and procedural measures are carried out as such:

- Limited to expressly authorized persons, with identification at the time of access and registration thereof, including filming by CCTV.
- Access to the rooms is done with ID card readers and managed by a computer system that keeps a log of inputs and outputs automatically.
- To access the rack where the cryptographic processes are located, prior authorization is necessary to have the key to open the cage.

### 5.2.2 Electrical Power and Air Conditioning

The facilities have current-stabilising equipment and power system doubled with generator equipment.

The rooms housing IT equipment have temperature control systems with air conditioners.

### 5.2.3 Exposure to water

The facilities are located in an area of low risk of flooding.

The rooms where computers are housed have a moisture detection system.

### 5.2.4 Fire prevention and protection

The facilities and assets have automatic detection and firefighting systems.

### 5.2.5 Backup Storage

Only authorized individuals have access to support storage.

The most highly classified information is stored in a safe offsite Data Processing Centre.



## Certification practice statement for timestamping service Público

### 5.2.6 Waste Management

The elimination of media, both paper and magnetic, is made by mechanisms that guarantee the impossibility of retrieving information.

In the case of magnetic media, it proceeds to formatting, permanent deletion, or physical destruction of the support. For paper documents, paper shredders or specially arranged bins for later destruction are used, under supervision.

### 5.2.7 Offline Backup

It is available a secure external storage for the safekeeping of documents, magnetic and electronic devices that are independent of the operations center.

## 5.3 Procedure Controls

It is guaranteed that its systems are operated safely, for which it has establish and implemented procedures for the functions which affect the supply of its services.

The staff runs the administrative and management procedures according to the security policy procedures.

### 5.3.1 Trust Roles

It is identified, according with its security policy, the following trust functions and roles:

- Internal Auditor: Responsible for compliance with operating procedures. This is an external person to the Department of Information Systems. The tasks of Internal Auditor are incompatible in time with tasks and incompatible with Certification Systems. These functions will be subordinate to the head of operations, reporting both this technical direction.
- System Administrator: Responsible for the proper functioning of hardware and software support platform certification.
- System Operator: Responsible, together with the Systems Administrator, for the correct functioning of the hardware and software supporting the certification platform. The operator is responsible for backup procedures and maintenance of the daily operations of the systems.
- Security Manager: Responsible for coordinating, monitoring and enforcing security measures as defined by the security policies of UANATACA. This individual should be responsible for aspects related to information security: logic, physics, networking, organization, etc.



## Certification practice statement for timestamping service

Público

Persons holding previous posts are subject to procedures of investigation and specific control. Additionally, it is applied a policy criteria for the segregation of duties, as preventive measure to fraudulent activities.

### 5.3.2 Identification and authentication for each role

The individuals assigned for each role are identified by the internal auditor will ensure that each person performs the operations for which they are assigned.

Each person only controls the assets required for its role, ensuring that no person access unallocated resources.

Access to resources is performed depending on the asset through cryptographic cards and activation codes.

### 5.3.3 Roles requiring separation of task

Trust roles are established under the principle of minimum privilege, ensuring a segregation of functions, so that the person holding a role does not have total or especially extensive control of all certification functions, ensuring due control and surveillance, limiting thus any type of fraudulent behavior internally.

The granting of the minimum privilege for trust functions will be done considering the best development of the activity and will be as limited as possible, considering the organizational structure at all times.

## 5.4 Personnel Controls

### 5.4.1 History, qualification, experience and authorization requirements

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

Staff in positions of trust has no personal interests that conflict with the development of the role that has been entrusted.

In general, TECALIS withdraws an employee from their duties when knowledge of the existence of the commission of any criminal act that could affect the performance of its functions.

TECALIS does not assign to a reliable site management a person who is not suitable for the position, especially for having been convicted of a crime or minor affecting their suitability for the position. For this reason, a previous investigation, to the extent permitted by applicable law, on the following is done:

- Studies, including alleged degree.



## Certification practice statement for timestamping service Público

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

### 5.4.2 Procedures of history investigation

Before hiring a person or before that person has access to the job, performs the following checks:

- References of the past years jobs
- Professional references
- Studies, including qualifications.

TECALIS obtains the unequivocal consent of the affected to such previous research, and processes and protects all his personal data in accordance with General Data Protection Regulation and every national regulations applicable.

All checks are made up to be allowed by the applicable law. The reasons that may lead the candidate rejection of a job are the followings:

- Falsehoods on the job application, done by the candidate.
- Very negative professional references or not very reliable.

### 5.4.3 Training requirements

TECALIS trains the staff in reliable and management jobs, until they reach the required qualification, keeping reports of the training.

Training programs are updated and improved periodically.

Training includes, at least, the following contents:

- Principles and mechanisms of security of the certification hierarchy, and the user environment of the person to train.
- Tasks the person must do.
- Policies and security procedures of TECALIS. Use and operation of machinery and installed applications.
- Management and processing of incidents and security compromise.
- Procedures of business continuity and emergency.
- Process management and security regarding the processing of personal data.

### 5.4.4 Retraining frequency and requirements

TECALIS, updates the staff training in accordance with the needs, and with enough frequency to comply their functions in a competent and satisfactory way, especially when doing the substantial modifications in the certification tasks.



## Certification practice statement for timestamping service Público

### 5.4.5 Job rotation frequency and sequence

N/A

### 5.4.6 Santions and authorized action

TECALIS has a disciplinary system, to debug the responsibilities arising from unauthorized actions, appropriate to the applicable labor legislation.

Disciplinary actions include suspension and loss of employment of the person responsible for the harmful action, proportionate to the gravity of the unauthorized action.

### 5.4.7 Professional contracting requirements

The staff hired to perform reliable tasks sign a previous confidentiality agreement and the operational requirements used by TECALIS. Any action that may compromise the security of the accepted processes could, once evaluated, lead to the termination of the employment contract.

In case all or part of the certification services were performed by a third party, the provisions and controls performed in this section, or other parts of the Certification Practice Statement, will be applied and complied by the third party who performs the operation functions of the certification services, notwithstanding, the certification authority will be responsible in any case for the effective implementation. These aspects are concretized in the legal instrument used to arrange the certification services provision by a third party different than TECALIS.

### 5.4.8 Documentation supplied to personnel

The certification services provider will provide the documentation strictly needed by the staff at any moment, to perform their job in a competent and satisfactory form.

## 5.5 Security Audit Procedures

### 5.5.1 Types of recorded events

It is produced and safely registered, at least, of the following events related to the entity security:

- Booting and shutting down of systems.
- Attempts to create, delete, set passwords or change privileges.
- Attempts to login and logout.
- Attempted unauthorized access to the TSA system through the network.
- Attempts of unauthorized access to the file system.
- Physical access to the logs.



## Certification practice statement for timestamping service

Público

- Changes in the configuration and maintenance of the system.
- Records of TSA applications.
- Turning on and off the TSA application.
- Changes in the details of the TSA and / or its codes.
- Records of the destruction of the media containing the keys, activation data.
- Events related to the life cycle of the cryptographic module, such as receiving, using and uninstalling it.
- The key generation ceremony and the key management databases.
- Physical access records.
- Maintenance and system configuration changes.
- Staff changes.
- Commitments and discrepancies reports.
- Records of the destruction of material containing key information, activation data or personal information of the subscriber, in case of individual certificates, or of the natural person identified in the certificate, in case of organization certificates.
- Complete reports of physical intrusion attempts in the infrastructures that support the service.
- Events related to synchronization and recalibration of the clock.

Log entries include the following elements:

- Login date and time.
- Serial number or entry sequence, in the automatic records.
- Identity of the entity entering in the register.
- Type of entrance.

### 5.5.2 Frequency of processing Audit Logs

It is reviewed its logs when a system alert motivated by the existence of any incident occurs.

Processing audit logs is a review of the records including the verification that confirm they have not been tampered, a brief inspection of all log entries and a deeper investigation of any alert or irregularities in the logs. The actions from the audit review are documented.

It is kept a system that guarantees:

- Enough space for logs storage.
- Logs files are not rewritten.
- Information held includes, at least: type of event, date and time, user running the event and result of the operation.
- Logs files will be held in structured files susceptible to incorporate into a DB for further exploration.



## Certification practice statement for timestamping service Público

### 5.5.3 Period of retention of audit logs

It is held the logs information for a period of between 1 and 15 years, depending on the type of information recorded.

### 5.5.4 Audit logs protection

The systems logs:

- Are protected from manipulation by signing the files that contain them.
- Are stored in fireproof devices.
- Availability is protected through its storage in facilities out of the center where the CA is located.

Access to logs files is reserved only to authorized persons. Also, devices are handled at all times by authorized personnel.

There is an internal procedure where management processes devices containing the data of the audit logs are detailed.

### 5.5.5 Audit log backup procedures

There is a proper backup procedure so that, in case of loss or destruction of relevant files, were available in a short period of time the corresponding logs backup.

It is implemented a secure backup procedure of audit logs, making a copy of all logs weekly in an external source. Additionally, a copy is held in a custody external center.

### 5.5.6 Location of the audit logs storage system

The information of the audit events is collected internally and in an automated way by the operating system, network communications and software certificate management, in addition to the data generated manually, will be stored by the authorized personnel. All this composes the storage system of audit logs.

### 5.5.7 Notification of the audit event to the subject that caused the event

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

### 5.5.8 Vulnerability analysis

The audit processes cover vulnerability analysis. Vulnerability analysis must be run, reviewed and revised by an examination of these monitored events. This analysis must be run daily, monthly and annually in accordance with the internal procedure intended for this purpose.





## Certification practice statement for timestamping service Público

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

### 5.6 Information Files

#### 5.6.1 Retention period for the files

It is saved the mentioned logs above for at least 15 years, or the period defined in the current law.

#### 5.6.2 Protection of the file

The file is protected so only the duly authorized persons can access to it. The file is protected against visualization, modification erased or any other manipulation through its storage in a reliable system.

It is ensured a proper protection of the files by assigning qualified personnel for its treatment and its storage in secure fireproof boxes and external facilities.

#### 5.6.3 File Backup procedures

There is an external storage center to ensure the availability of the file backups of electronic files. The physical documents are stored in safe places restricted to authorized personnel.

At least, It is made incremental daily backups of support of all its electronic documents and makes weekly full backups for data recovery cases.

In addition, in cases where there is a need to keep a copy of the documents on paper, they are stored in a safe place.

#### 5.6.4 Requirements of timestamping

Records are dated with a reliable source via NTP.

There is no need to sign this information digitally.

#### 5.6.5 Location of the file system

It is available a centralized system of gathering information of the activity of the equipment involved in the certificate management service.



## **Certification practice statement for timestamping service**

Público

### 5.6.6 Procedures to obtain and verify file information

It is available a procedure where describes the process to verify that the stored information is correct and reachable. TECALIS provides the information and means of verification to the auditor.

## 5.7 Key Renewal

Each key pair of the TSU Certificates used for the time stamping service is associated with the system that provides such service. Prior to the use of the private key of the TSU certificate expire, a key change is made before the expiration or revision of the current ones.

## 5.8 Compromised Key and Disaster Recovery

### 5.8.1 Management procedures of incidents and compromise

It is developed security policies and business continuity, which allows the management and backup of the systems in case of compromise or disaster of its operations.

### 5.8.2 Resources, applications or data corruption

When resources, applications or data corruption events happen, the proper management procedures will begin, which contemplate scaling, investigation and response to the incident. Procedures of compromise of the keys or disaster recovery will begin, if necessary.

### 5.8.3 Compromised private key of the entity

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

### 5.8.4 Business continuity capabilities after a disaster

It will be restored the critical services in accordance with the contingency and business continuity plan restoring the normal operation of the previous services within 24 hours of the disaster.

It is available an alternative center for the operation of certification schemes described in the business continuity plan, if necessary.

## 5.9 Service Termination

TECALIS ensures that possible interruptions to subscribers of the service and to third parties are minimal as a consequence of the cessation of the services of the certification service



## Certification practice statement for timestamping service Público

provider. In this sense, TECALIS 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, TECALIS will execute all actions necessary to transfer to a third party or a notarial repository, the maintenance obligations of the specified records during the corresponding period according to this Time Stamping Certification Practices Statement or the corresponding legal forecast.

Before the services cessation, TECALIS develops a termination plan, with the following provisions:

- Provide the necessary funds, including civil liability insurance, to continue the completion of the revocation activities.
- Inform all Subscribers of the service, Third party that they trust and, in general, any third party with whom they have agreements or other type of termination relationship with a minimum anticipation of 3 months.
- Destroy or disable for use the private keys in charge of the time-stamping service.
- Execute the tasks necessary to transfer the maintenance obligations of the registration information and the event log files during the respective time periods.
- Communicate to the corresponding Spanish Supervisory Body, at least 3 months in advance, the cessation of its activity.
- Likewise, it will inform you of the opening of any bankruptcy proceeding against TECALIS, as well as any other relevant circumstance that may prevent the continuation of the activity.



## Certification practice statement for timestamping service Público

### 6. Technical Security Controls

In the provision of trust services, reliable systems and products are used, protected against any alteration and that guarantee the technical and cryptographic security of the certification, which are used as support.

#### 6.1 Generation and Installation of Their Pair Keys

##### 6.1.1 Generation of the key pair

The key pair of the TSU Certificate is generated by the Trust Service Provider Uanataca, S.A., in accordance with its Certification Practices Statement and its disclosure text, available on the website: [www.uanataca.com](http://www.uanataca.com).

Likewise, the 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. These records are kept for audit and monitoring purposes during an appropriate period determined by TECALIS.

To generate the intermediate key, devices with Common Criteria EAL4+ certification are used, specifically the following: nShield Solo XC Hardware Security Module v12.60.15 for the SSCD.

The keys are generated using the RSA public key algorithm, with a minimum length of 3072 bits.

|                  |             |               |
|------------------|-------------|---------------|
| TSU certificates | 2.3072 bits | Up to 8 years |
|------------------|-------------|---------------|

\*TECALIS may continue to use the TSU with 2048-bit RSA keys until the Ministry approves the new 3072-bit TSU, and in any case, until December 31, 2026.

##### 6.1.2 Sending of the public key to the certificate issuer

The method of remission of the public key to the relying electronic certification services provider is PKCS#10, other equivalent cryptographic test or any other method approved by TECALIS.

##### 6.1.3 Public key distribution of the certification services provider

TECALIS's keys are communicated to third parties who trust in certificates, ensuring the integrity of the key and authenticating its origin, through its publication in the Deposit.



## Certification practice statement for timestamping service

Público

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

The certificate of the CA root and subordinated will be available on the UANATACA web page.

### 6.1.4 Key Sizes

- The key length for the Root Certification Authority is 4,096 bits.
- The key length for the Subordinate Certification Authority is 4,096 bits.
- The key length for the TSU Certificates is 3,072 bits.
- \*tecalís may continue to use the TSU 01 certificate with 2,048-bit RSA keys until the Ministry approves the new TSU certificate, and in any case, at most until December 31, 2026.

### 6.1.5 Generation of public key parameters

The TSU certificates public key are encrypted in accordance with RFC 5280.

### 6.1.6 Quality check of the public key parameters

- Module Length= 3072 bits
- Algorithm of keys generation: rsagen1
- Cryptographic functions of Summary: SHA256.
- \*tecalís may continue to use the TSU 01 certificate with 2,048-bit RSA keys until the Ministry approves the new TSU certificate, and in any case, at most until December 31, 2026.

### 6.1.7 Key generation in IT applications or in equipment goods

All keys are generated in equipment goods, in accordance with the indicated in section 6.1.1.

### 6.1.8. Hash Algorithms Used in the Service

- Hash used on the data to be time stamped:



## Certification practice statement for timestamping service Público

- The identifier of the hash algorithm used to generate the evidence fingerprint. In this case, the allowed algorithms are:
  - SHA-256 (secure hash ALGORITHM 256-bit OID: 2.16.840.1.101.3.4.2.1)
  - SHA-384 (secure hash ALGORITHM 384-bit OID: 2.16.840.1.101.3.4.2.2)
  - SHA-512 (secure hash ALGORITHM 512-bit OID: 2.16.840.1.101.3.4.2.3)
- The time stamp signature algorithm:
  - In this case, the algorithm used is RSA (SHA256rsa 1.2.840.113549.1.1.11).

## 6.2 Private Key Protection

### 6.2.1 Cryptographic modules standards

The modules that manage the keys of TECALIS are compliant with the certification FIPS 140-2 level 3 and Common Criteria EAL4+.

### 6.2.2 Private key multi-person (n of m) control

A multi-person control is required for activating the private key of the TSU Certificate. In case of this Certification Practice Statement, in detail there is a policy of 3 of 6 persons for the keys activation.

Cryptographic devices are physically protected, as determined in this document.

### 6.2.3 Private key backup

It is made a backup copy of the TSU certificate private key that makes their recovery in case of disaster, loss or deterioration thereof. Both generation of the copy and the recovery thereof need at least two people participation.

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

### 6.2.4 Private key transfer into a cryptographic module

Private keys are directly generated in the cryptographic modules in the public key infrastructure.

The private keys of the TSU Certificates are stored encrypted in the cryptographic modules of the public key infrastructure.



## Certification practice statement for timestamping service Público

### 6.2.5 Method of activating the private key

The private key management procedures of the TECALIS's TSU Certificate is activated by executing the corresponding secure start procedure of the cryptographic module, by people who perform reliable functions.

### 6.2.6 Method of deactivating the private key

Before destroying the keys, a revocation of the certificate of the public keys associated with them will be issued.

Devices that have stored any part of TECALIS private keys are physically destroyed or reset to low level. For disposal, the same steps outlined in the corresponding manual of the cryptographic equipment are followed.

Finally, the backups will be destroyed in a safety way.

### 6.2.7 Cryptographic modules classification

See section 6.2.

## 6.3 Computer Security Controls

It is used reliable systems to provide certification services. It has made controls and computer audits to establish its proper computer activity management with the level of security required in the system management of electronic certification.

Regarding the information security, UANATACA as the Public Key Infrastructure provider applies the certification scheme controls on management systems ISO 27001.

Used equipment's are initially configured with appropriate security profiles of UANATACA staff system, in the following aspects:

- Setting up the operating system.
- Setting up the application security.
- Correct sizing of the system.
- User and permissions settings.
- Setting event Log.
- Backup and recovery plan.
- Antivirus settings.
- Requirements of network traffic.

Each server includes the following features:

- Imposition of separation of tasks for the management of privileges.



## Certification practice statement for timestamping service Público

- Identification and authentication of roles associated with identities.
- Audit of events related to security.
- Key recovery mechanisms and the TSA system.

The exposed functionalities are realized through a combination of operating system, PKI software, physical protection and procedures.

### 6.4 Life Cycle Technical Controls

#### 6.4.1 System development controls

The applications are developed and implemented in accordance with the development and change control standards.

The applications have methods for verifying the integrity and authenticity, as well as the correction of the version to use.

#### 6.4.2 Security management controls

It is developed activities for training and employee awareness of security. The materials used for training and descriptive documents processes are updates after approval by a group for security management. An annual training plan is used.

It is required by contract security measures equivalent to any external provider involved in the certification tasks of the relying electronic service.

##### **6.4.2.1 Classification and management of information and goods**

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

There is a security policy details the procedures of information management where it is classified according to its level of confidentiality.

The documents are classified into three levels: UNCLASSIFIED, INTERNAL USE and CONFIDENTIAL.

##### **6.4.2.2 Management Operations**

There is an appropriate process management and incident response, by implementing a warning system and the generation of periodic reports.

In the security document the incident management process is developed in detail.





## Certification practice statement for timestamping service Público

TECALIS has documented all the procedure relative to the roles and responsibilities of the staff involved in the control and manipulation of elements contained in the certification process.

### **6.4.2.3 Treatment of support and safety**

All supports are treated safely in accordance with the requirements of the classification of information. The supports that contain sensitive information are destroyed safely if they are not going to be required again.

### **6.4.2.4 Planning Systems**

Systems department keeps track of the capabilities of the equipment. In conjunction with the implementation of resources control each system can provide a possible downsizing.

### **6.4.2.5 Reports of incidents and response**

There is a procedure for follow-up of incidents and its resolution, where the answers and an economic evaluation are registered, which supposes the resolution of the incident.

### **6.4.2.6 Operational proceedings and Liabilities**

It is defined activities assigned to persons with a role of trust, other than those responsible for performing daily operations that do not have character of confidentiality.

### **6.4.2.7 Access system management**

It is made all efforts that are reasonable available to confirm that the system access is limited to authorized persons.

In particular:

- There are controls based on firewalls, antivirus and IDS in high availability.
- Sensitive data is protected by cryptographic techniques or access controls with strong identification.
- A data management procedure is taken into account.
- Procedures are in place to ensure that operations are respected in the role policy.
- Each person has a role to perform the certification operations.
- The staff is responsible for their actions through the commitment of confidentiality with the company.

### **6.4.2.8 Life cycle management of cryptographic hardware**



## Certification practice statement for timestamping service Público

TECALIS ensures that the cryptographic hardware used for signing certificates is not handled during its transport by inspecting the delivered material.

The cryptographic hardware moves on prepared supports to prevent any manipulation.

It is recorded all relevant device information to add to the catalogue of assets.

The use of cryptographic hardware for signature certificates requires the use of at least two trusted employees.

It is made periodic tests to ensure the correct functionality of the device.

Only reliable personnel manipulate the cryptographic hardware device.

TECALIS TSU Certificate private key stored in the cryptographic hardware will be erased once the device is removed.

The system configuration, as well as its modifications and updates are documented and controlled.

Changes or updates are authorized by the security officer and they are reflected in the corresponding team's working minutes. At least, two reliable persons perform these settings.

### 6.5 Engineering controls of Cryptographic Modules

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

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

All cryptographic operations are performed in modules with FIPS 140-2 level 3 certification.

### 6.6 Time Sources

It is available a procedure of time synchronization coordinated via NTP, that has access to two independent services:

- The first synchronization is a service based on GPS antennas and receivers that allow a level of trust of STRATUM 1 (with two high availability systems).
- The second one has a complementary synchronization, via NTP, with the Spanish Royal Institute and Observatory of the Navy (ROA).



## Certification practice statement for timestamping service Público

### 6.7 Electronic Qualified Time Stamp Time Accuracy

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

TECALIS has a reliable source of time in high availability that allows a confidence level of STRATUM 1, via NTP, with the CSUC.

The accuracy of the TECALIS Qualified Time Stamping service is 1 second with respect to UTC.

### 6.8 Change of State of a Qualified Signature Creation Device (SSCD)

In the case of modification of the status of the certification of the qualified signature creation devices (SSCD) that support the provision of trust services, the following procedure will be followed:

1. A list of certified SSCDs is available, as well as a close relationship with suppliers of said devices, in order to guarantee alternatives to possible loss of certification status of SSCD devices.
2. In the event of termination of the period of validity or loss of certification, said SSCDs will not be used for the provision of the time-stamping service.
3. Proceed immediately to change to SSCD devices with valid certification.
4. In the event that it is proven that a SSCD device has never been a qualified device, either by falsification or any type of fraud, it will proceed immediately to inform the clients and the national regulator about the revocation of the electronics certificates issued by these devices. Subsequently it will proceed to replace them by a valid SSCD device.



## Certification practice statement for timestamping service Público

### 7. TSU Certificate Profile

The TSU certificate profile for the provision of the time stamp service follows the processes and indications established in the Certification Practice Statements (CPS) of UANATACA and its disclosure text (PDS), all available on the website: <https://web.uanataca.com/>

#### 7.1 Certificate Profile

The TSU Certificates are compliant with the standard X.509 version 3, RFC 3739 and the ETSI EN 319 422.

##### 7.1.1 Version Number

The certificate is X.509 Version 3.

##### 7.1.2 Certificate extensions

Certificates extensions are detailed in the profile's documents, which are accessible from UANATACA's web (<https://www.uanataca.com>).

In this way, it is allowed to keep more stable versions of the Certification Practice Statement and decouple them from frequent adjustments in the profiles.

##### 7.1.3 Object Identifier (OID) of the algorithms

The object identifier of the signature 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



## Certification practice statement for timestamping service Público

### 7.1.4 Names Format

Certificates must contain the required information for its use, as determined by the appropriate policy.

### 7.1.5 Names Restriction

The names in the certificates are restricted to “Distinguished Names” X.500, that are unique and non ambiguous.

### 7.1.6 Object Identifiers (OID) of certificates types

All certificates include an identifier of the certificates policy under which they have been issued.

## 7.2 Certificate Revocation List Profile

The procedure of revocation, suspension and / or reactivation of TSU certificates follow the processes and indications established in the Certification Practice Statement and Disclosure Text (PDS) of UANATACA, all available on the website: <https://web.uanataca.com/>

### 7.2.1 Version Number

CRLs issued by UANATACA are from version 2.

### 7.2.2 OCSP profile

According to standard IETF RFC 6960.



## Certification practice statement for timestamping service Público

### 8. Compliance Audit

TECALIS has communicated the beginning of its activity as a trust service provider by the National Supervisory Body, currently the Ministry of Industry, Trade and Tourism, and is subject to the control reviews that this body considers necessary.

#### 8.1 Frequency of Compliance Audit

TECALIS conducts a compliance audit annually, in addition to internal audits carried out at its own discretion or at any time, due to a suspected breach of any security measure.

#### 8.2 Identification and Qualification of the Auditor

An external independent audit signature performs the audits, demonstrating technical competence and experience in computer security, information systems security and compliance audits of public key certification services and related elements.

#### 8.3 Auditor Relationship to Audited Entity

Audit firms are of renowned prestige, with specialized departments in conducting IT audits, so there is no conflict of interest that could undermine its performance in relation to TECALIS.

#### 8.4 Topics Covered by Audit

The Audit verifies with reference to TECALIS that:

- The entity has a management system, which ensures the quality of service.
- The entity complies with the requirements of the Certification Practice Statement and other documentation related to the issuance of the various digital certificates.
- The Certification Practice Statement and other related legal documentation comply with the agreed with TECALIS and the established in the current regulation.
- The entity properly manages its information systems.



## Certification practice statement for timestamping service Público

### 8.4 Actions taken as a result of Lack of Conformity

Once the management has received the auditor's compliance report, the deficiencies found are analyzed with the audit entity. This report also develops and implements the corrective policies that tackle these deficiencies.

If TECALIS is unable to develop and/or implement the corrective measures or if the deficiencies found suppose an immediate threat to the system security or integrity, shall immediately inform to the security responsible which can perform the following actions:

- Cease operation temporarily.
- Revoke the TSU certificate key and regenerate the infrastructure.
- Terminate the TSA service.
- Other complementary actions needed.

### 8.5 Treatment of Audit Reports

The audit reports are delivered to the responsible team of the security in a timelimit of 15 days after the audit.



## Certification practice statement for timestamping service Público

### 9. Business and Legal Requirements

#### 9.1 Fees

##### 9.1.1 Timestamping service fees

TECALIS can establish a fee for the time-stamping service, from which, if applicable, the subscribers will be informed in a timely manner.

##### 9.1.2 Timestamping status information Access fees

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

##### 9.1.3 Fees for other services

Not Stipulated.

##### 9.1.4 Refund Policy

Not Stipulated.

#### 9.2 Financial Capacity

TECALIS has enough economic resources to keep its operations, to comply with its obligations and to confront the risk of liability for claim and damages, as established in the applicable regulation, in relation to the management of the services finalization and termination plan.

##### 9.2.1 Cobertura de seguro

TECALIS has warranty coverage of its civil liability, with an insurance of professional civil liability that complies with the current regulation applicable.

##### 9.2.2 Other assets

Not Stipulated.

##### 9.2.3 Insurance Coverage for subscribers and relaying third parties in certificates

TECALIS has a warranty coverage of its civil liability, with an insurance of professional civil liability, for relaying electronic services, with the minimum insured of 1,500,000 Euros.





## Certification practice statement for timestamping service

Público

### 9.3 Confidentiality

#### 9.3.1 Confidential Information

The following information is kept confidential by TECALIS:

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

#### 9.3.2 Legal disclosure of information

TECALIS only discloses the confidential information in the cases legally foreseen.

### 9.4 Personal Data Protection

TECALIS is compliance with current regulations on the protection of personal data, as reflected in the General Data Protection Regulation No. 2016/679 and in general any applicable national regulations.

In compliance with, TECALIS has documented in this Certification Practice Statement the security and organizational aspects and procedures, in order to guarantee that all the personal data to which it has access are protected against its loss, destruction, damage, forgery and illegal or unauthorized processing.

The following is a detail of all the necessary information regarding the processing of personal data made by TECALIS:

#### **Data Controller**

The personal data given by reason of the Service would be treated by TECALIS SOFTWARE SL, who is configured as the Data Controller and whose data are detailed here:

Tecalis Software S.L.

B70186184

Rúa Oliveira 35, Parque empresarial Novo Milladoiro, 15895 Milladoiro-Ames,

A Coruña, España

+34 911 01 07 00



## Certification practice statement for timestamping service

Público

[hello@tecalis.com](mailto:hello@tecalis.com)

### Purposes of data processing

TECALIS processes the personal data provided in order to carry out the requested electronic services, specifically the issuance of electronic certificates, all in accordance with the provisions of the TECALIS Certification Practice Statement (CPS), which is available at the following link: <https://www.tecalis.com/es/politicas-sellado-tiempo>.

The purposes of data processing related to the SERVICE are the following:

- Identification of service subscribers.
- Communications regarding the service.
- Custody and maintenance of the records associated with the service.
- Administrative, accounting, and billing management arising from the contracting of the service.

### Lawfulness of processing

In accordance with the indicated data purposes, the legal basis for the treatment of personal data of users is:

- The legitimation of the data processing for the provision of electronic trust services is the execution of the contract for the services requested, where the user is part of it.

### Processed data and conservation

The categories of personal data processed by UANATACA include, but are not limited to:

- Identification data: first name, last name, and official identification number.
- Professional data: organization, department, and/or job title.
- Contact data: postal address, email address, and telephone number.

Personal data will be retained until the termination of the contractual relationship and, subsequently, for the legally required periods applicable to each case. As a general rule, personal data related to the service will be retained for 15 years following the termination of the contract or provision of the service.



## Certification practice statement for timestamping service

Público

### Data transfer

Data may be made available to third parties within the territory of the European Union in connection with the provision of services contracted by the user (for example, data hosting providers (data centers), identification support services, group companies, etc.), all pursuant to the corresponding data processing agreement, guaranteeing appropriate security measures at all times to ensure the proper protection of users' personal data.

Notwithstanding the foregoing, as a general rule, personal data will only be disclosed to third parties under legal obligation.

As a general rule, no international data transfers will be carried out.

### User Rights

Users may exercise their rights of confirmation, access, rectification, erasure, cancellation, restriction of processing, objection, and data portability.

- Confirmation: All users have the right to obtain confirmation as to whether TECALIS is processing personal data concerning them.
- Access and Rectification: Users have the right to access all their personal data, as well as to request the rectification of any inaccurate or incorrect data.
- Erasure and Cancellation: Users may request the erasure/cancellation of their data when, among other reasons, the data is no longer necessary for the purposes for which it was collected.
- Restriction and Objection: Users may request the restriction of processing so that their personal data is not applied to the corresponding operations. Under certain circumstances and for reasons related to their particular situation, users may object to the processing of their data, in which case TECALIS will be obligated to cease processing it, except for compelling legitimate grounds, or the exercise or defense of potential legal claims.
- Portability: Data subjects may request that their personal data be sent to them or transmitted to another controller in a structured, commonly used electronic format.

To exercise their rights, users may send a request to the email address [hello@tecalis.com](mailto:hello@tecalis.com) or write to the following postal address:

Rúa Oliveira 35, Parque empresarial Novo Milladoiro,

15895 Milladoiro-Ames,



## Certification practice statement for timestamping service Público

A Coruña, Spain

In said request, they must attach a copy of their identity document and clearly state which right they wish to exercise.

### 9.5 Intellectual Property Rights

TECALIS is the only one that has intellectual property rights of this Certification Practice Statement.

### 9.6 Obligations and Civil Liability

TECALIS goza de derechos de propiedad intelectual sobre esta Declaración de Prácticas de Certificación de Sellado de Tiempo.

#### 9.6.1 TECALIS Obligations

TECALIS guarantees, under full responsibility that complies with all requirements established in the Certification Practice Statement, and it is responsible for ensuring compliance with the procedures described, according to the instructions contained in this document.

TECALIS provides relying electronic services in accordance with this Certification Practice Statement.

TECALIS informs the subscriber of the terms and conditions related to the use of the certificate, price and use limitations, through a subscriber contract that includes by reference the disclosure texts (PDS) of each of the acquired certificates.

The disclosure text document, also known as PDS, meets the content of Annex A of ETSI EN 319 411-1 v1.1 (2016-02) this document can be transmitted by electronic media, using a sustainable communication method, and in accessible language.

TECALIS binds subscribers, key holders and third parties that trust in certificates through the disclosure text or PDS, in written and understandable language, with the minimum following contents:

- Requirements to comply with the provisions established in this document.
- Limits on the use of time stamps.
- Information on how to validate a time stamp, including the requirement to check the status of the stamp, and the conditions under which it can reasonably be relied upon, which is applicable when the subscriber acts as a trusted third party.



## Certification practice statement for timestamping service Público

- The way in which the liability of the Certification Authority is guaranteed.
- Limitations of liability, including the uses for which the Certification Services Provider accepts or excludes liability.
- Period of archiving audit records.
- Applicable dispute resolution procedures.
- Applicable law and competent jurisdiction.

### 9.6.2 Guarantees offered to subscribers and relying third parties in certificates

TECALIS in the documentation between subscribers and third parties that trust, establishes and rejects guarantees, and applicable limitations of liability.

TECALIS guarantees the subscriber that the time stamps comply with all the material requirements established in this Certification Practice Statement, as well as the reference standards.

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

### 9.6.3 Rejection of other guarantees

TECALIS rejects any other guarantee that is not enforceable under the laws, except those contemplated in this document.

### 9.6.4 Limitation of liability

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

TECALIS does not perform any verification of the document for which the Time Stamp is requested, since it is sent directly by the Subscriber under its own and exclusive responsibility.

TECALIS does not assume any 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.

TECALIS will not be responsible for any direct damage and / or by third parties because of the misuse of the qualified time stamps duly issued in accordance with this document.



## Certification practice statement for timestamping service Público

### 9.6.5 Fortuitous event and force majeure

TECALIS includes in the disclosure text or PDS, clauses that limit its responsibility in fortuitous event or force majeure.

### 9.6.6 Applicable Law

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

### 9.6.7 Severability, survival, entire agreement and notification clauses

TECALIS establishes, in the subscriber's contract and in the disclosure text or PDS, the 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 remain in force after the completion of the regulatory service of the legal relationship between the parties. For this purpose, the Certification Authority ensures that the requirements of sections 9.6.1 (Obligations and liability), 8 (Compliance audit) and 9.3 (Confidentiality), remain in force after the termination of the service and the general conditions of issuance/use.
- Under the entire agreement clause it is understood that the regulatory legal service contains the full will and all agreements between the parties.
- Under the notification clause, it will be established the procedure by which the parties mutually report incidents.

### 9.6.8 Competent Jurisdiction Clause

TECALIS establishes, in the subscriber's contract and in the disclosure text or PDS, a jurisdiction clause, indicating that the international jurisdiction corresponds to the Spanish judges.

The territorial and functional jurisdiction shall be determined under the regulations of international private law and procedural law that may be applied.

### 9.6.9 Resolution of conflicts

TECALIS establishes, in the subscriber's contract, and in the disclosure text or PDS, mediation and resolution procedures of applicable disputes.



# **Certification practice statement for timestamping service**

Público

## 10. Annex I - Acronyms

|      |                                                                                                                   |
|------|-------------------------------------------------------------------------------------------------------------------|
| AC   | Autoridad de Certificación. Certification Authority                                                               |
| CA   | Certification Authority. Autoridad de Certificación                                                               |
| RA   | Autoridad de Registro. Register Authority                                                                         |
| CN   | Common Name                                                                                                       |
| CP   | Certificate Policy                                                                                                |
| CPD  | Centro de Procesamiento de Datos. Data Processing Center                                                          |
| CPS  | Certification Practice Statement. Declaración de Prácticas de Certificación                                       |
| CRL  | Certificate Revocation List. Lista de certificados revocados                                                      |
| CSR  | Certificate Signing Request. Petición de firma de certificado                                                     |
| DES  | Data Encryption Standard. Estándar de cifrado de datos                                                            |
| DN   | Distinguished Name. Nombre distintivo dentro del certificado digital                                              |
| DPC  | Declaración de Prácticas de Certificación. Certification Practice Statement                                       |
| DSA  | Digital Signature Algorithm. Estándar de algoritmo de firma                                                       |
| DCCF | Dispositivo Cualificado de Creación de Firma. Qualified Signature Creation Device                                 |
| ETSI | European Telecommunications Standards Institute o Instituto Europeo de Normas de Telecomunicaciones               |
| QSCD | Qualified Signature Creation Device. Dispositivo Cualificado de Creación de Firma                                 |
| FIPS | Federal Information Processing Standard Publication. Publicación estándar de procesamiento de información federal |
| ISO  | International Organization for Standardization. Organismo Internacional de Estandarización                        |
| LRC  | Listas de Revocación de Certificados. Certificate Revocation Lists                                                |
| LDAP | Lightweight Directory Access Protocol. Protocolo de acceso a directorios                                          |





## Certification practice statement for timestamping service

Público

|        |                                                                                            |
|--------|--------------------------------------------------------------------------------------------|
| NTP    | Network Time Protocol. Protocolo de tiempo de red                                          |
| OCSP   | On-line Certificate Status Protocol. Protocolo de acceso al estado de los certificados     |
| OID    | Object Identifier. Identificador de objeto                                                 |
| PA     | Policy Authority. Autoridad de Políticas                                                   |
| PC     | Política de Certificación. Certification Policy                                            |
| PDS    | Texto de divulgación – Policy Disclosure Statement                                         |
| PIN    | Personal Identification Number. Número de identificación personal                          |
| PKCS   | Public-Key Cryptography Standards. Estándares de criptografía de clave pública             |
| PKI    | Public Key Infrastructure. Infraestructura de clave pública                                |
| PSC    | Prestador de Servicios Electrónicos de Certificación / Confianza. Trust Services Provider. |
| RSA    | Rivest-Shimar-Adleman. Tipo de algoritmo de cifrado                                        |
| SHA    | Secure Hash Algorithm. Algoritmo seguro de Hash                                            |
| SSL    | Secure Sockets Layer                                                                       |
| TCP/IP | Transmission Control. Protocol/Internet Protocol                                           |
| TSA    | Autoridad de Sellado de Tiempo – Time Stamping authority                                   |
| TSP    | Trust Service Provider. Prestador de Servicios Electrónicos de Certificación / Confianza   |
| TSU    | Unidad de Sellado de Tiempo – Time Stamping Unit                                           |