



**ENTRUST EU S.L.**

***eIDAS Qualified Time-stamp Authority Practice Statement***

Version: 1.1

December 1, 2023

© 2023 Entrust EU S.L. All rights reserved.

## Revision History

Issue	Date	Changes in this Revision
1.0	September 1, 2022	Initial version.
1.1	December 1, 2023	Update security policy reference

## TABLE OF CONTENTS

<i>Introduction</i> .....	4
<b>1. Scope</b> .....	<b>5</b>
<b>2. References</b> .....	<b>6</b>
<b>3. Definitions and abbreviations</b> .....	<b>7</b>
<b>3.1 Definitions</b> .....	<b>7</b>
<b>3.2 Abbreviations</b> .....	<b>8</b>
<b>4. General concepts</b> .....	<b>9</b>
<b>4.1 General policy requirements concepts</b> .....	<b>9</b>
<b>4.2 Time-stamping services</b> .....	<b>9</b>
<b>4.3 Time-Stamping Authority (TSA)</b> .....	<b>9</b>
<b>4.4 Subscriber</b> .....	<b>10</b>
<b>4.5 Time-stamp policy and TSA practice statement</b> .....	<b>10</b>
<b>5. Introduction to time-stamp policies and general requirements</b> .....	<b>11</b>
<b>5.1 General</b> .....	<b>11</b>
<b>5.2 Identification</b> .....	<b>11</b>
<b>5.3 User community and applicability</b> .....	<b>11</b>
Best practices time-stamp policy.....	11
<b>6. Policies and practices</b> .....	<b>12</b>
<b>6.1 Risk assessment</b> .....	<b>12</b>
<b>6.2 Trust Service Practice Statement</b> .....	<b>12</b>
<b>6.2.1 Time-stamp format</b> .....	<b>12</b>
<b>6.2.2 Accuracy of the time</b> .....	<b>12</b>
<b>6.2.3 Limitations on the use of the time-stamping service</b> .....	<b>12</b>
<b>6.2.4 Obligations of the subscriber</b> .....	<b>12</b>
<b>6.2.5 Obligations of relying parties</b> .....	<b>13</b>
<b>6.2.6 Verification of the time-stamp</b> .....	<b>13</b>
<b>6.2.6.1 Verification of the time-stamp issuer</b> .....	<b>13</b>
<b>6.2.6.2 Verification of the time-stamp revocation status</b> .....	<b>13</b>
<b>6.2.7 Applicable law</b> .....	<b>13</b>
<b>6.2.8 Service availability</b> .....	<b>13</b>
<b>6.3 Terms and conditions</b> .....	<b>13</b>

6.4	Information security policy.....	13
6.5	TSA obligations.....	14
6.5.1	General .....	14
6.5.2	TSA obligations towards subscribers .....	14
6.6	Information for relying parties .....	14
7.	<i>TSA management and operation</i> .....	15
7.1	Introduction .....	15
7.2	Internal organization.....	15
7.3	Personnel security.....	15
7.4	Asset management .....	15
7.5	Access control.....	15
7.6	Cryptographic controls .....	16
7.6.1	General .....	16
7.6.2	TSU key pair generation .....	16
7.6.3	TSU private key protection.....	16
7.6.4	TSU public key certificate.....	16
7.6.5	Rekeying TSU's key.....	17
7.6.6	Life cycle management of signing cryptographic hardware.....	17
7.6.7	End of TSU key life cycle .....	17
7.7	Time-stamping .....	17
7.7.1	Time-stamp issuance .....	17
7.7.2	Clock synchronization with UTC.....	18
7.8	Physical and environmental security .....	18
7.9	Operation security .....	18
7.10	Network security.....	18
7.11	Incident management .....	18
7.12	Collection of evidence.....	18
7.13	Business continuity management .....	19
7.14	TSA termination and termination plans.....	19
7.15	Compliance.....	19
8.	<i>Additional requirements for qualified time-stamps</i> .....	20
8.1	TSU public key certificate.....	20

**8.2 TSA issuing non-qualified and qualified electronic time-stamps.....20**

## Introduction

This Time-stamping Authority Practice Statement (TPS) applies to the eIDAS Qualified Time-Stamping Services of Entrust EU S.L. (“Entrust”).

The qualified Time-stamps comply with the requirements set by the “Regulation (EU) No. 910/2014” of the European Parliament (eIDAS throughout this document).

The eIDAS Qualified Timestamping Service terms and conditions are determined by the overall Entrust Certification Practice Statement (CPS) for Qualified Certificates.

This document states only additional Time-stamping specific practices; in particular, the facility, management and operational controls, security measures, processes and procedures which have been implemented to satisfy the requirements of eIDAS and other relevant international standards for Time-stamping Authorities. An independent conformity assessment body verifies the efficiency of these procedures on a regular basis.

This document is structured according to ETSI EN 319 421 “Policy and Security Requirements for Trust Service Providers issuing Time-Stamps”.

## 1. Scope

This document specifies policy and security requirements relating to the operation and management practices of the Entrust Qualified Time-Stamp Authority issuing Time-stamps. Such Time-stamps can be used in support of digital signatures or for any application requiring to prove that a datum existed before a particular time.

The present document can be used by independent bodies as the basis for confirming Entrust can be trusted for issuing qualified Time-stamps according to eIDAS.

This and other Entrust related documents referenced within this document are available online at <https://entrust.net/cps>.

## 2. References

For the purposes of this document, the standards referenced in the Entrust CPS for Qualified Certificates and the following apply:

- ETSI EN 319 401: General Policy Requirements for Trust Service Providers
- ETSI EN 319 421: Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
- ETSI EN 319 422: Time-stamping protocol and Time-stamp token profiles
- RFC 3161: Internet X.509 Public Key Infrastructure Time-stamp Protocol (TSP)
- RFC 1305: Network Time Protocol



### 3. Definitions and abbreviations

#### 3.1 Definitions

For the purposes of this document, the terms and definitions given in the Entrust CPS for Qualified Certificates and the following apply:

**Coordinated Universal Time (UTC):** time scale based on the second as defined in Recommendation ITU-R TF.460-6

**Relying Party:** recipient of a Time-stamp who relies on that Time-stamp

**Subscriber:** legal or natural person to whom a Time-stamp is issued and who is bound to any Subscriber obligations

**Time-stamp:** data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time

**Time-stamp policy:** named set of rules that indicates the applicability of a Time-stamp to a particular community and/or class of application with common security requirements

**Time-Stamping Authority (TSA):** TSP providing Time-stamping services using one or more Time-stamping Units

**Time-stamping service:** trust service for issuing Time-stamps

**Time-Stamping Unit (TSU):** set of hardware and software which is managed as a unit and has a single Time-stamp signing key active at a time

**Trust Service:** electronic service that enhances trust and confidence in electronic transactions

**Trust Service Provider (TSP):** entity which provides one or more trust services

**TSA Disclosure statement:** set of statements about the policies and practices of a TSA that particularly require emphasis or disclosure to Subscribers and relying parties, for example to meet regulatory requirements

**TSA practice statement:** statement of the practices that a TSA employs in issuing Time-stamp

**TSA system:** composition of IT products and components organized to support the provision of Time-stamping services

**UTC(k):** time scale realized by the laboratory "k" and kept in close agreement with UTC, with the goal to reach  $\pm 100$  ns.

### 3.2 Abbreviations

For the purposes of this document, the abbreviations given in the Entrust CPS for Qualified Certificates and the following apply:

BIPM	Bureau International des Poids et Mesures
BTSP	Best practices Time-Stamp Policy
CA	Certification Authority
GMT	Greenwich Mean Time
IERS	International Earth Rotation and Reference System Service
IT	Information Technology
TAI	International Atomic Time
TPS	Time-stamp Authority Practice Statement
TSA	Time-Stamping Authority
TSP	Trust Service Provider
TSU	Time-Stamping Unit
UTC	Coordinated Universal Time

## 4. General concepts

### 4.1 General policy requirements concepts

This document references ETSI EN 319 401 for generic policy requirements common to all classes of trust service providers service.

These policy requirements are based upon the use of Public Key cryptography, Public Key certificates and reliable time sources.

Subscriber and relying parties are expected to consult this TPS to obtain further details of precisely how this Time-stamp policy is implemented by the particular TSA (e.g. protocols used in providing this service).

### 4.2 Time-stamping services

The provision of Time-stamping services is broken down in this document into the following component services for the purposes of classifying requirements:

- **Time-stamping provision:** This service component generates Time-stamps.
- **Time-stamping management:** This service component monitors and controls the operation of the Time-stamping services to ensure that the service provided is as specified by the TSA. This service component has responsibility for the installation and de-installation of the Time-stamping provision service.

### 4.3 Time-Stamping Authority (TSA)

A Trust Service Provider (TSP) providing Time-stamping services to the public, is called the Time-Stamping Authority (TSA). The TSA has overall responsibility for the provision of the Time-stamping services identified in clause 4.2. The TSA has responsibility for the operation of one or more TSUs which creates and signs on behalf of the TSA.

The TSA may make use of other parties to provide parts of the Time-stamping services. However, the TSA always maintains overall responsibility (as per clause 6.5) and ensures that the policy requirements identified in this document are met.

#### **4.4 Subscriber**

When the Subscriber is an organization, it comprises several end-users or an individual end-user and some of the obligations that apply to that organization will have to apply as well to the end-users. In any case the organization will be held responsible if the obligations from the end-users are not correctly fulfilled and therefore such an organization is expected to suitably inform its end users.

When the Subscriber is an end-user, the end-user will be held directly responsible if its obligations are not correctly fulfilled.

#### **4.5 Time-stamp policy and TSA practice statement**

This clause explains the relative roles of Time-stamp policy and this TPS. It places no restriction on the form of a Time-stamp policy or practice statement specification.

A Time-stamp policy is a form of Trust Service Policy as specified in ETSI EN 319 401 applicable to trust service providers issuing Time-stamps.

The TPS is a form of Trust Service Practice Statement as specified in ETSI EN 319 401 applicable to trust service providers issuing Time-stamps.

This TPS specifies a Time-stamp policy and practice statement for the Entrust TSA.

## 5. Introduction to time-stamp policies and general requirements

### 5.1 General

This document defines a set of rules adhered to by Entrust when issuing Time-stamps, supported by Public Key certificates, with an accuracy of one (1) second or better against UTC.

### 5.2 Identification

The identifier of the Time-stamp policy specified in this document is:

```
itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023) policy-  
identifiers(1) best-practices-ts-policy (1)
```

By including one of these object identifiers in a Time-stamp, the TSA claims conformance to the identified Time-stamp policy.

### 5.3 User community and applicability

#### **Best practices Time-stamp policy**

This policy is aimed at meeting the requirements of Time-stamp for long term validity but is generally applicable to any use which has a requirement for equivalent quality.

This policy may be used for public Time-stamping services or Time-stamping services used within a closed community.

## **6. Policies and practices**

### **6.1 Risk assessment**

See section 5.4.8 of the Entrust CPS for Qualified Certificates.

### **6.2 Trust Service Practice Statement**

Entrust ensures the quality, performance and operation of the Time-stamping service through the implementation of various security policies and controls.

The security policies and controls are reviewed regularly by an independent body, whilst trained trustworthy personnel check the adherence of the security controls to the policies.

#### **6.2.1 Time-stamp format**

The issued Time-stamps are compliant to RFC 3161 and ETSI EN 319 422. The service issues RSA 4096 Time-stamps that uses the SHA256 hash algorithm. The service accepts Time-stamp requests with SHA256, SHA384 or SHA512 hash algorithms.

#### **6.2.2 Accuracy of the time**

The Time-stamping service uses a reliable time source from a set of UTC(k) laboratory NTP servers and monitors the drift from these sources using an NTP time monitor.

The Time-stamping service reaches an accuracy of the time well under +/-1s with respect to UTC.

Note that the time of Time-stamping is not the timestamping request acceptance moment, but the timestamping system processing moment.

#### **6.2.3 Limitations on the use of the time-stamping service**

No stipulation.

#### **6.2.4 Obligations of the subscriber**

Subscribers must verify that the Time-stamp token has been correctly signed and check the Entrust EU validation services (i.e., CRL or OCSP) to confirm the Time-stamp certificate has not been revoked.

Subscribers must use secure cryptographic functions for Time-stamping requests or software to create Time-stamps.

If a Subscriber exhausted its quota and the server returns a "429 Too Many Requests" HTTP status the Subscriber must respect the "Retry-After" HTTP header.

Please see the Subscriber Agreement for additional information.

### **6.2.5 Obligations of relying parties**

Before relying on a Time-stamp the Relying Party must verify that the Time-stamp has been correctly signed and Time-stamp certificate was not revoked at time of signature.

### **6.2.6 Verification of the time-stamp**

#### **6.2.6.1 Verification of the time-stamp issuer**

The Public Keys of the used certificates, including the TSU and CA certificates, are published to enable a verification that the Time-stamp has been signed correctly by the TSA.

#### **6.2.6.2 Verification of the time-stamp revocation status**

The validity Public Keys of the used certificates, including the TSU and CA certificates must be checked using the CRL or OCSP responder included in those certificates.

### **6.2.7 Applicable law**

See section 9.14 of the Entrust CPS for Qualified Certificates.

### **6.2.8 Service availability**

Entrust has implemented the following measures to ensure availability of the service:

- Redundant setup of IT Systems, including HSM infrastructure, in order to avoid single points of failure
- Redundant facilities in order to avoid loss of service
- Use of uninterruptable power supplies

Entrust aims to provide 99.9% service availability per year.

### **6.3 Terms and conditions**

See chapter 9 of the Entrust CPS for Qualified Certificates.

### **6.4 Information security policy**

See section 5.3.8 of the Entrust CPS for Qualified Certificates.

## **6.5 TSA obligations**

### **6.5.1 General**

Entrust is responsible for:

- The compliance with this TPS and its internal or published policies and procedures.
- The compliance with applicable laws and regulations.

### **6.5.2 TSA obligations towards subscribers**

This TPS does not place any specific obligations on the Subscriber beyond those stated in the Subscriber Agreement.

## **6.6 Information for relying parties**

The obligations of Relying Parties are covered in the Relying Party agreement. In addition, the Relying Party shall do the following:

- verify that the Time-stamp has been correctly signed and that the Private Key used to sign the Time-stamp has not been compromised until the time of the verification;
- take into account any limitations on the usage of the Time-stamp indicated by the Time-stamp policy; and
- take into account any other precautions prescribed in agreements or elsewhere.



## 7. TSA management and operation

### 7.1 Introduction

Entrust has implemented information security policies and operational procedures to maintain the security of the service.

### 7.2 Internal organization

For the proper operations of the Time-stamping service, Entrust maintains non-disclosed documentation that specifies all operational controls concerning personnel security, access controls, risk assessment etc. These internal documents are used by independent bodies to confirm compliance of the service against ETSI EN 319 421.

- a) The TSA is provided by: Entrust
- b) Information security management and quality management of the service is carried out within the security concept of the service.
- c) The TSA has employed sufficient personnel with the necessary education, training, technical knowledge and experience to manage and operate the Time-stamping service.

### 7.3 Personnel security

See section 5.3 of the Entrust CPS for Qualified Certificates.

### 7.4 Asset management

All information and physical assets associated with information-processing facilities used within the service are clearly identified, categorized and filed in accordance with Entrust Asset Management Policy.

### 7.5 Access control

Different security layers with respect to physical access and logical access ensure a secure operation of the Time-stamping service.

Access to information, information processing facilities and business processes must be controlled based on the Entrust Access Control Policy. This policy considers:

- Access to network and network services
- User access management, including:
  - Registration, de-registration and provisioning
  - Privileged access rights

- Segregation of duties
- Review of access rights
- Removal or adjustment of access rights
- Responsibilities
- System and application access control, including:
  - Information access restrictions
  - Secure log-on procedures
  - Password management system
  - Use of privileged utility programs
  - Access control to program source code

## 7.6 Cryptographic controls

### 7.6.1 General

See section 6.2 of the Entrust CPS for Qualified Certificates.

### 7.6.2 TSU key pair generation

TSU Key Pair generation is performed per section 6.1.1.3 of the Entrust CPS for Qualified Certificates. The TSU Key Pair generation algorithm, key length and signature algorithm is specified in the Entrust CPS for Qualified Certificates.

The TSU Private Key will not be imported into different cryptographic modules. The TSU only has one active Private Key at a time.

### 7.6.3 TSU private key protection

See section 6.2 of the Entrust CPS for Qualified Certificates.

### 7.6.4 TSU public key certificate

Entrust guarantees the integrity and authenticity of the TSU signature verification (public) keys as follows:

- TSU signature verification (public) keys are available to relying parties in publicly available certificates. The certificates can be found on the Entrust's website at <https://entrust.net/cps>
- The TSU does not issue a Time-stamp before its signature verification (Public Key) certificate is loaded into the TSU or its cryptographic device. When obtaining a signature verification (Public Key) certificate, Entrust verifies that this certificate has been correctly signed (including verification of the certificate chain to its trusted certification authority).

### 7.6.5 Rekeying TSU's key

The validity period of TSU's certificate shall not be longer than the period of time that the chosen algorithm and key length is recognized as being fit for purpose. The TSU's certificate validity period is specified in section 6.3.2 of the Entrust CPS for Qualified Certificates.

### 7.6.6 Life cycle management of signing cryptographic hardware

Trusted Role personnel will inspect cryptographic hardware during the commissioning process to ensure integrity and there has been no evidence of tampering found while stored.

Installation, activation and duplication of TSU's signing keys in cryptographic hardware shall be done only by personnel in Trusted Roles using dual control in a physically secured environment.

TSU Private Keys stored on TSU cryptographic module are erased upon device retirement.

### 7.6.7 End of TSU key life cycle

The usage period of the TSU Private Key is per section 6.3.2 of the Entrust CPS for Qualified Certificates. The Private Keys usage period will not exceed the validity of certificates issued using those Private Keys.

After the end of the Private Key usage period, the Private Keys within the cryptographic hardware are destroyed in a manner such that the Private Keys cannot be retrieved or used anymore.

## 7.7 Time-stamping

### 7.7.1 Time-stamp issuance

The Entrust Qualified Time-stamping Service issues qualified Time-stamps as follows:

- Time-stamps conform to the timestamp profile defined in ETSI EN 319 422.
- Time-stamps include the correct time, which is traceable to at least one real time values distributed by a UTC(k) laboratory.
- Time synchronization and accuracy issues are address in section 7.7.2 of this document.
- If the Time-stamp clock is detected as being outside of the stated accuracy, then Time-stamps will not be issued.
- Time-stamps are signed with a key generated specifically for this purpose.
- Time-stamp service will not issue Time-stamps beyond the validity period of the Private Key.

### 7.7.2 Clock synchronization with UTC

The TSU clock is synchronized with UTC as specified in section 6.2.2 of this document, specifically:

- TSU clocks are maintained such that the clocks do not drift outside the declared accuracy.
- Declared accuracy is 1 second or better.
- TSU clocks are protected against threats which could result in an undetected change to the clock that takes it outside its calibration.
- The TSA detects if the time that would be indicated in a Time-stamp drifts or jumps out of synchronization with UTC.
- If it is detected that the time that would be indicated in a Time-stamp drifts or jumps out of synchronization with UTC, the TSU will stop time-stamp issuance.
- The clock synchronization is maintained when a leap second occurs as notified by the appropriate body and the change to take account of the leap second occurs during the last minute of the day when the leap second is scheduled to occur. A record will be maintained of the exact time (within the declared accuracy) when this change occurred.

### 7.8 Physical and environmental security

See section 5.1 of the Entrust CPS for Qualified certificates.

### 7.9 Operation security

See chapter 5 of the Entrust CPS for Qualified certificates.

### 7.10 Network security

See chapter 5 of the Entrust CPS for Qualified certificates.

### 7.11 Incident management

See section 5.7.1 of the Entrust CPS for Qualified certificates.

### 7.12 Collection of evidence

See sections 5.4 and 5.5 of the Entrust CPS for Qualified certificates.

In addition the following evidence is collected:

- Synchronization of a TSU's clock to UTC
- Records concerning all events relating to detection of loss of synchronization

### **7.13 Business continuity management**

See section 5.7 of the Entrust CPS for Qualified certificates.

### **7.14 TSA termination and termination plans**

See section 5.8 of the Entrust CPS for Qualified certificates.

In addition when the TSA terminates its services, the TSA shall revoke the TSU's certificates.

### **7.15 Compliance**

Entrust ensures compliance with applicable law at all times.

Specifically, the Entrust TSA is compliant to:

- a) REGULATION (EU) No. 910/2014
- b) ETSI EN 319 401, ETSI EN 319 421, ETSI EN 319 422
- c) IETF RFC 3161

Entrust maintains its compliance with the eIDAS standards identified above via a Qualified Auditor on a bi-annual (eIDAS) and continuous basis. The audit is performed by a conformity assessment body accredited by a European Union member state national accreditation body on the basis of EN ISO/IEC 17065 as profiled by ETSI EN 319 403 and in particular against the requirements defined in the eIDAS Regulation (EU) No 910/2014.

## **8. Additional requirements for qualified time-stamps**

### **8.1 TSU public key certificate**

The TSU certificate will be issued from a CA which meets the QCP-1 and BTSP policy.

The Private Keys of the TSU certificates will sign qualified Time-stamps as indicated by the qcStatement “esi4-qtstStatement-1”.

### **8.2 TSA issuing non-qualified and qualified electronic time-stamps**

The TSUs will not issue non-qualified electronic Time-stamps.