TIME STAMP POLICY (TSA)

ZIURTAPEN ETA ZERBITZU ENPRESA-EMPRESA DE CERTIFICACION Y SERVIC

Firmado digitalmente por ZIURTAPEN ETA ZERBITZU ENPRESA-EMPRESA DE CERTIFICACION Y SERVIC
Fecha: 2022.10.17 08:00:20 +02'00'

TRACK CHANGES

VERSION	DATE	CHANGE
1.1	20/02/2018	– 5.1. Identification. Update of the policy identifier. Time stamp token: 1.3.6.1.4.1.14777.3.3
1.2	06 October 2021	– A new heading is included: Change Control, and document DOC_P_Update_DPTSA is deleted. – The wording is improved. – 5.1. Identification. Update of the policy identifier. Time stamp token: 1.3.6.1.4.1.14777.300.1 – 6.5 Time stamp issue procedure. Subordinate Certification Authority Certification Chain Update CN = SUBCA QC IZENPE – TSA – 6.8.3 TSA certificate profile Updating of certificate data. – 6.8.4 Time stamp token profile. OID Update OID = 1.3.6.1.4.1.14777.300.1
1.3	04/10/2022	- 6.8.2 section: profile of a timestamp request. Specification of supported hash algorithms.

Table of contents

Content

1 INTRODUCTION

Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, S.A. (hereinafter, Izenpe) offers a qualified time stamp service as part of its services as qualified trust service provision, according to the definition in European Parliament and Council Regulation (EU) Number 910/2014, dated 23 July 2014, on electronic identification and trust services for electronic transactions on the domestic market, repealing Directive 1999/93/EC (hereinafter, eIDAS).

This service creates and records digital proof of the existence of data at a determined instant on the timeline, in a trustworthy and reliable fashion, significantly improving the reliability of electronic data.

Izenpe created a Time Stamp Authority (TSA) to provide the time stamp service.

This document describes the Time Stamp Authority (TSA) policy, specifying the time stamp authority's general policies and processes to create the time stamp and its services. Technical details and processes in addition to Izenpe's Certification Practice Statement (CPS) are specified.

The procedures defined and proper implementation are audited by an external entity, according to specifications defined by ETSI by means of standard EN 319 421.

2 DEFINITIONS AND ACRONYMS

2.1 Definitions

This Policy refers to the definitions and acronyms used in the Certification Practice Statement, in addition to:

- Time Stamp Authority (TSA): authority that issues time stamp tokens
- Third-party users: user who trusts a time stamp provided by Izenpe
- Subscriber: person who uses the services provided by the TSA and explicitly accepts the terms and conditions
- Time stamp policy: rules that apply to the TSA when a time stamp token is created
- Time stamp token: data object that links the existence of digital data to a specific moment. This acts as proof that a piece of data existed at a determined instant on the timeline.
- Time stamp unit: hardware and software components managed as one unit that provide time stamp tokens from one sole source of time. Components can be cloned or deployed in redundancy to achieve high availability.
- Declaration of TSA Practises: TSA's policies and practises, especially oriented toward subscribers and third parties.
- Coordinated Universal Time**:** solar time at the prime meridian (0º). The time scale is based on the second, as defined in ETSI TS 102.023 and in ITU-R Recommendation TF.460-5.
- UTC(k): time scale made by laboratory 'k' according to UTC, with the purpose of attaining maximum deviation of +-100ns.

2.2 Acronyms

- TSA: Time Stamp Authority
- TSU: Time Stamp Unit
- TST: Time Stamp Token
- UTC: Coordinated Universal Time
- eIDAS: European Parliament and Council Regulation (EU) Number 910/2014 dated 23 July 2014 on electronic identification and trust services for electronic transactions on the domestic market, repealing Directive 1999/93/EC
- DTSAP: Declaration of TSA Practises
- CPS: Certification Practices Statement

3 SCOPE

This document defines the TSA operational and management practises so that trust subscribers and third parties can assess the trustworthiness of time stamp services.

The TSA's policy requirements meet stipulations in European Regulation eIDAS. Izenpe's time stamp services may be used with an electronic signature or any application that requires proof of the existence of digital data a specific point in time. These policy requirements are based on public-key cryptography, public-key certifications (X.509) and reliable time sources.

This document, along with Izenpe's CPS, may be used by independent entities to assess this TSA's trustworthiness, as well as its time stamp services.

4 GENERAL CONCEPTS

4.1 Time stamp services

The time stamp services include two components:

- Providing time stamps: technical component responsible for generating time stamp tokens
- Time stamp administration: component of the service that monitors and controls operation of time stamp services. Managing the time stamp guarantees that the clocks used for the time stamp are correctly synchronised with UTC.

4.2 Time Stamp Authority

Izenpe's TSA issues secure time stamp tokens (TST) for time stamp service users (for example, subscribers or third parties).

Izenpe's TSA assumes all responsibility for providing the time stamp services indicated in section "14 Responsibilities ". Izenpe's TSA may operate several different identification time stamp units (TSUs) and each TSU may have a different key (see section "6.8.4 Time stamp token profile").

Keys may be cloned within one TSU and be used with redundant components to meet high-availability requirements.

Izenpe's TSA is identified in the digital certificate used by time stamp services. The profile is available in section "6.8.3 TSA certificate profile".

4.3 Subscriber

The subscriber may be an organisation or an individual.

- If the subscriber is an organisation, the obligations applicable to said organisation are also applicable to its associated end users.

  The organisation shall adequately inform its end users, being responsible if the end users do not properly fulfil the obligations.
- If the subscriber is an individual user, the end user shall be directly responsible for fulfilling the obligations.

4.4 Time stamp policy and Declaration of TSA Practises

4.4.1 Purpose

The Time Stamp Policy and Statement of Practice are defined as:

- The TSA Policy defines the aspects that must be fulfilled both by the subscriber and the Authority issuing the time stamps. The rules and processes applied by TSA when a time stamp token is generated are included.
- The Declaration of Practises (CPS) is a statement of how the time stamp service is implemented in order to fulfil the policy's requirements.
- To complement the processes described in Izenpe's CPS, this TSA policy describes specific policies and processes.

4.4.2 Degree of specificity

The TSA policy specifies the processes used to provide time stamp services, extending the processes described in the CPS.

4.4.3 Focus

The TSA policy focuses on general processes: technical details such as the organisational structure, operational procedures and communications infrastructure are specified in the CPS or in internal documents. The internal documents are not available to the public.

5 INTRODUCTION TO TSA POLICY AND GENERAL REQUIREMENTS

5.1 Identification

Izenpe includes the following policy identifier (OID) to all time stamp tokens issued by the TSA.

Time stamp token	1.3.6.1.4.1.14777.300.1

5.2 User community and applicability

Time stamp service users will be subscribers and third parties who require the service. There is a limitation on the number of monthly requests, with an associated cost for the service. Contact Izenpe to see conditions and rates.

5.3 Compliance

Compliance with this Time Stamp Policy is subject to independent periodical audits, both internal and external.

Izenpe complies with the obligations defined in section 'Obligations and Responsibilities' and ensures implementation of the appropriate controls.

6 TIME STAMP POLICY

6.1 Roll-out and maintenance of trust systems

The keys to the TSA and its services are produced in a trusted environment. The systems and products used by Izenpe provide appropriate services according to the assurance levels required. Izenpe guarantees that it carries out an appropriate analysis of security requirements and has change control procedures.

6.2 Time Stamp Policy

The TSA operates in services according to the rules established in this Policy, the CPS and additional internal documents that define technical, operational, and procedural requirements. At its discretion, Izenpe may offer specific TSA services to a petitioner.

The Policy defines how Izenpe heeds to the requirements identified in the CPS and other internal documents.

The procedures defined and their correct implementation and audited on a yearly basis by an independent external entity.

The TSA and other relevant documentation is available at www.izenpe.eus

The TSA Disclosure Statement is included in point '6.2.2 TSA Disclosure Practices Statement.' Internal documents are not published. Modifications to TSA practises or any other document published are implemented according to CPS specifications.

The terms and conditions established in this document are binding for all subscribers and third parties using Izenpe's time stamp services.

Other documents that complement this Policy such as the CPS may be found at www.izenpe.eus

- Izenpe's TSA is a qualified time stamp service, according to eIDAS
- For contact information, see section '1.5.2 Contact information' in the CPS
- Obligations of the entity issuing time stamps are defined in section 6.3.1 *Time Stamp Issuing Entity Obligations* in this document
- Obligations of the subscriber are defined in point 6.3.2 *Time stamp subscriber obligations* in this document
- Obligations of third parties are defined in point 6.3.3 *Obligations of third parties verifying time stamps* in this document
- Responsibilities of the Time Stamp Authority are defined in point 6.4 *Responsibilities* in this document
- The service bears a cost according to Izenpe's price catalogue rates.
- Izenpe keeps records on all TSA operations, as indicated in point 6.13 *Collection of evidence* in this document.
- For possible complaints and to resolve disputes, see point 9.12 *Complains and dispute resolution* in the CPS.
- Subscribers and third parties accept the conditions of use defined by Izenpe

- Izenpe's TSA certificate is issued by a Certification Authority whose certification policy follows the guidelines stipulated in Izenpe's CPS.
- Each time stamp token issued by Izenpe's TSA service includes the object identifier defined in section 6.8.4 *Time stamp token profile*.
- Hash algorithms permitted are indicated in section 6.8.2 *Time stamp request profile.* The TSA token signature algorithm is defined in section 6.8.4 *Time stamp token profile*.
- The TSA ensures time precision compatible with minim UTC time standards at +/-1 second. Izenpe's TSA does not issue time stamp tokens if said precision cannot be guaranteed.
- Responsibility limitations are defined in section 6.4 *Responsibilities* in this document, in the CPS and in other service agreements held with users.

6.3 Obligations and responsibilities

Izenpe, as an Entity that issues time stamps according to this Policy, undertakes the following obligations:

6.3.1 Time Stamp Issuing Entity Obligations

The Izenpe Time Stamp Authority,

- issues secure time stamp tokens (TST) for time stamp service users (including both subscribers and third parties).
- Undertakes the responsibility of providing time stamp services.
- May operate with different time stamp identifiable units (TSUs), each one of which may have its own signature key.
- Is identified in the digital certificate used by time stamp services.
- Offers its services to all subscribers and third parties verifying time stamps that commit to fulfil their obligations.

6.3.2 Time stamp subscriber obligations

The time stamp subscriber may use the Time Stamp Service only as specified by ETSI EN 319 422.

The subscriber must verify that the time-stamp token has been properly signed by the time-stamping authority, and that the private key used to sign the time-stamp token has not been revoked.

The subscriber must fulfil the current Izenpe Timestamping Policy, available at www.izenpe.eus

6.3.3 Obligations of third parties verifying time stamps

When a time stamp token is received, the third party must verify that the token is correctly signed and that the private key used to sign the time stamp has not been revoked.

As long as the certificate used to generate time stamps is not expired, its validity may be verified in the matching CRL.

In the event that verification is performed after the certificate's validity period has expired, the third party must verify that the hash function used, the algorithms and the length of the cryptographic keys may be deemed secure.

6.4 Responsibilities

- Izenpe operates its TSA according to Izenpe's TSA policy, its CPS, and the terms of any other binding agreement between Izenpe and time stamp service users.
- Izenpe tries to provide high availability in its services, but it does not offer a total availability guarantee, nor does it guarantee precision in the time stamps. Izenpe is not responsible under any circumstances for profit losses, indirect or consequent harm, or data loss, insofar as valid legislation allows.
- Izenpe shall not be held responsible for harm as a result of infractions committed by the subscriber or third parties regarding applicable terms and conditions.
- Under no circumstances shall Izenpe be held responsible for harm as the result of force majeure events such as natural disasters, electrical or telecommunications blackouts, fire, non-foreseeable external interactions such as viruses or hacker attacks, governmental attacks or strikes.
- In any event, Izenpe shall take all reasonable measures to mitigate the effects of such events. Any harm that is the consequence of a delay caused by a force majeure event shall not be covered by Izenpe.

6.5 Time stamp issue procedure

In order to provide the Time Stamp Service, Izenpe manages the corresponding keys as described in section 6.7 *Cryptographic controls* in this document.

The Time Stamps issued under this policy are signed by specific certificates, issued under the Certification Chain of the root Certification Authority with CN = SUBCA QC IZENPE - TSA.

For more information on the above-mentioned root Certification Authority Certification Chain see section 1.3.1 CPS Certification Authorities.

6.5.1 Time stamp service provision and availability

The Time Stamp shall be issued at the behest of the user entity. When this entity wishes to obtain a Time Stamp for an electronic document, it shall calculate a value or set of hash values based on it. This shall be included in a time stamp request structure and shall be sent to Izenpe so that it can issue the corresponding Time Stamp.

This Time Stamp shall link the data received and reception date and time through Izenpe's electronic signature.

Accepted algorithms are described in section 6.8.2 *Time stamp request profile* in this document.

Izenpe shall not perform any verification or handle how the data received to be stamped is represented beyond including it in the Time Stamp and the event record systems. Izenpe shall not verify the content in any way, nor the veracity of how the data to be stamped is represented, nor its origin.

The Time Stamp Service is available twenty-four (24) hours per day, every day of the year, except for circumstances beyond Izenpe's control or during maintenance operations. The latter circumstance shall be notified by Izenpe sufficiently beforehand, and an attempt will be made to resolve it in a period no longer than twenty-four (24) hours.

Both Time Stamp requests and responses are managed as described in recommendation IETF RFC 3161.

6.5.2 Time stamp request

Time Stamp requests are sent to the address http://tsa.izenpe.com, encapsulated as Content-Type: application/timestamp-query, encoded in DER and described in ASN.1 (See IETF RFC 3161)

6.5.3 Response to a time stamp request

Responses to a Digital Date request are received at the address http://tsa.izenpe.eus, encapsulated as Content-Type: application/timestamp-reply, encoded in DER and described in ASN.1.

The response content is an ASN.1 structure that includes the result of the operation (status). In other words, if the operation was performed in satisfactory fashion or not, and a CMSSignedData structure (timeStamp Token) including the digital date (TSTInfo), signed by the Digital Date Authority.

The Digital Stamping Authority certificate is a certificate issued by the CA with the id-kp-timestamping extension, indicating that this certificate will be used for the exclusive purpose of dating digital documents.

6.6 TSA administration and operation

6.6.1 Security Management

Management of Izenpe's TSA security is described in section 5. *Physical, procedural and staff security controls* in the CPS.

6.6.2 Archive classification and management

Izenpe's TSA ensures that the information and other assets are appropriately handled regarding security, as defined in section 5.7 *Contingency Plan* in the CPS.

6.6.3 Staff security

Staff security controls are defined in section 5. *Physical, procedural and staff security controls* in the DCP.

6.7 Cryptographic controls

6.7.1 Creation of the TSA key

Izenpe creates the cryptographic keys in a physically secure environment, performed by trusted staff. Izenpe's TSA keys are created according to a specific procedure. The maximum duration for the TSA certificate is 5 years.

6.7.2 TSU private key protection

Izenpe's TSA guarantees the confidentiality and integrity of its keys. Particularly, the HSM meets FIPS 140-2 level 3 requirements and the EAL4+ assurance level for the corresponding profile. In this regard, TSA keys are kept with a security level equivalent to the level described in the CPS for Izenpe's subordinate CAs.

6.7.3 Distribution of the TSU public key

Izenpe's TSA certificate is posted on www.izenpe.eus.

6.7.4 Renewal with regeneration of the TSU key

Izenpe's TSA keys must be replaced before the certificate expires if the algorithm, length of the key or any other security measure is no longer deemed as reliable by the industry. In any event, the keys are regenerated, and a new certificate is issued every two years.

6.7.5 End of the TSU key's life cycle

Izenpe's TSA does not allow for signing timestamp responses with an expired or revoked certificate. In the event that Izenpe's TSA services finalise, all private keys from TSA certificates, including security copies, will be destroyed so that said keys are unrecoverable.

6.7.6 Managing the life cycle of the cryptographic module used to sign time stamps

Izenpe establishes procedures to guarantee that non-repudiation services for hardware security modules (HSM) are not handled during sending and storage.

Only trusted staff install and activate the signature keys contained in the cryptographic hardware. Operation, procedures, and life cycle management for HSM is described in Izenpe's internal documentation.

6.7.7 Compromised TSA certificate private key

In the event that an Izenpe TSA service private key is compromised, the procedure indicated in point 5.7.3 *Procedure in the event of compromise of a private key* in the CPS is applied.

In the event of compromise of an Izenpe TSA service private key, no timestamp tokens shall be issued.

In the event that the minimum precision of +/- 1 second is compromised, time stamps shall not be issued until calibration is corrected.

In the event that an Izenpe TSA service private key is compromised, relevant information will be posted for subscribers and third parties on Izenpe's webpage. Additionally, subscribers will be informed as soon as possible.

6.7.8 TSA Finalisation

Izenpe's TSA shall terminate according to procedures defined in section 5.8 *CA Termination* in the CPS.

6.8 Time stamp

6.8.1 Time source used to provide the service

Izenpe obtains the time for its systems from a connection to the Real Observatorio de la Armada (Royal Observatory of the Navy) (ROA), following the NTP protocol through the connection established with the Basque Government. A description of the NTP protocol may be found in the IETF RFC 5905 standard.

Based on this internal service, Izenpe offers a time stamp service (TSA) that may be used to create time stamps on arbitrary documents, according to IETF RFC 3161.

6.8.2 Time stamp request profile

- The time stamp request must follow the structure defined in IETF RFC 3161.
- The request must follow instructions in ETSI TS 101 861.
- Hash algorithms accepted are SHA1 and SHA2. In any event, Izenpe follows industry recommendations regarding cryptographic suites.

6.8.3 TSA certificate profile

TSA signature creation data is linked to the following Certificate:

EXTENSION ATTRIBUTE	VALUE	COMMENT
Subject	CN = tsa.izenpe.com 2.5.4.97 = VATES-A01337260 O = IZENPE S.A. C = ES	
Issuer Name	CN = SUBCA QC IZENPE - TSA 2.5.4.97 = VATES-A01337260 O = IZENPE S.A. C = ES	
Key Usage	Digital signature (80)	
Extended Key Usage	Date printing (1.3.6.1.5.5.7.3.8)	
Subject key Identifier	<key identifier of this CA's public key>	
Authority key identifier	<key identifier of the issuing CA's public key>	
CRL Distribution Point	http://crl.izenpe.eus/cgi-bin/izenpeTSA	URLs of the CRL Distribution points
Certificate Policy	[1]Certificates directive: Directive identifier=1.3.6.1.1.4.1.14777.10.1 [1.1]Directive certifier information: Directive certifier id=CPS Certifier: http://www.izenpe.eus/cps [1.2]Directive certifier information: Directive certifier id=User notice Certifier: Notice text = Kontsulta www.izenpe.eus-en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consult www.izenpe.eus for terms and conditions before using or relying on the certificate.	
Subject Information Access	[1]Access to authority information Access method=access method unknown (1.3.6.1.5.5.7.48.3) Alternative name: URL address=http://tsa.izenpe.eus/	

6.8.4 Time stamp token profile

- For the time stamp protocol, the IETF RFC 3161 and RFC 5816 standards are followed.
- For the stamp profile and policies, ETSI EN 319 421 (Policy and Security Requirements for Trust Service Providers issuing Timestamps) and ETSI EN 319 422 (Time-stamping protocol and time-stamp token profiles) standards are followed.
- All timestamp tokens issued by Izenpe include the policy identifier object (OID) 1.3.6.1.4.1.1.14777.300.1.
- All timestamp tokens issued by Izenpe include the Timestamp certificate used to sign the token.
- The certificate used to sign is generated with sha256WithRSAEncryption with a key length of 4096 bits, and is exclusively for use of the TSA service.
- The token's hash algorithm is SHA-256.

6.8.5 Clock synchronisation with UTC

- Izenpe's TSA uses its own time server, which is synchronised with the ROA (Real Observatorio de la Armada) (Royal Navy Observatory).
- There are controls to detect changes in calibration and/or synchronisation problems that can compromise the defined precision.
- The TSA ensures time precision compatible with minim UTC time standards at +/-1 second. Izenpe's TSA does not issue time stamp tokens if said precision cannot be guaranteed.
- Izenpe's TSA ensures proper handling of all leap seconds during the last minute of the day when the adjustment is scheduled.

6.9 Physical and environment security

Izenpe ensures the physical and environmental security of its TSA as defined in section 5. *Physical, procedural and staff security controls* in the CPS.

6.10 Operational management

Izenpe's TSA keeps appropriate operational controls according to guidelines in ETSI EN 319 421. These documents and policies are internal and are not available to the public. They are periodically verified by internal and external reviews to ensure their compliance and effectiveness.

6.11 Network security

The network's security is based on the concept of multi-level zoning with multiple redundant firewalls. The confidential information transferred by insecure networks is encrypted by using SSL/TLS protocols.

6.12 Incident management

As defined in section 5.7.1 *Incident management procedure* in the CPS.

6.13 Collection of evidence

As indicated in section 5.4 *CPS Audit*.

6.14 Archiving of information related to the operation of time-stamping services

Records related to time stamp service operation are generated and stored just like the records related to operation of the Certification Authority. Respective controls ensure the integrity, confidentiality and filing as required for all records as specified in section 5.5 *Filing Records* in the CPS.

Izenpe ensures that there are adequate measures to prevent inadequate record processing.

6.15 Managing access to systems

Izenpe's TSA has adequate access controls as defined in section 5. *Physical, procedural and staff security controls* in the CPS.

6.16 Compliance with legal requirements

Izenpe's TSA services comply with eIDAS requirements. Izenpe ensures that adequate measures are taken to prevent unauthorised handling of personal information. Izenpe also ensures the confidentiality of personal information and other information provided by users to the TSA.

6.17 Organisational

Izenpe's TSA organisation is the same as with subordinate CAs. The organisational security, technical and staff security measures are defined in the CPS and comply with other laws and regulations as defined in this policy.