Qualified Service Policy

QUALIFIED TIME-STAMPING AUTHORITY OF FIRMAPROFESIONAL (TSA)

Version: 201021

Clasification: Public

BARCELONA
EDIF. ESADECREAPOLIS
AV. TORRE BLANCA, 57 - LOCAL 386
08173 SANT CUGAT DEL VALLÈS
+34 934 774 245

MADRID
VELÁZQUEZ 59, 1º CTRO.-IZDA.
28001 MADRID
+34 915 762 181

WWW.FIRMAPROFESIONAL.COM

Use and disclosure restrictions of the document's content. .

Version History

Version	Section and changes	Publication date
6.0	To view changes from previous versions, please send an email to info@firmaprofesional.com	15/04/2014 (only Spanish)
170705	Change of template and version numbering, moving to YYMMDD (year, month and day of publication) format Adaptation to qualified service eIDAS.	05/07/2017 (only Spanish)
200226	Template change. Terminology inconsistency corrections: timestamp, Time-Stamping, etc. Clarifications made about custody. Added section 7.8. Calibration Loss Control Addition of the new time stamp data	26/02/2020
201021	TSA certificate update	21/10/2020

Index

1. Introduction

1.1. General description

Firmaprofesional, as a Trust Service Provider that issues qualified certificates according to 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 domestic market and so repealing Directive 1999/93 / EC, also offers Time-Stamping services.

The purpose of this document is to describe the operation of the Time-Stamping Services offered by Firmaprofesional and to establish the conditions of use, obligations and responsibilities of the various entities involved.

The aforementioned Regulation (EU 910/2014), includes and regulates the issue of time-stamps, defining them as "data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time".

In addition, it is the intention of Firmaprofesional to provide the issued time-stamps with the status of "Qualified Time-Stamps" by satisfying the requirements set out in Article 42 of Regulation (EU) 910/2014.

The present document is based on the regulation ETSI EN 319 421 "Policy and Security Requirements for Trust Service Providers issuing time-stamps" and the profiles are in accordance with regulation ETSI EN 319 422 "Time-stamping protocol and time-stamp token profiles".

This Time-Stamping Policy is subject to compliance with the General Conditions outlined in the **Certification Practices Statement** (CPS) of Firmaprofesional.

1.2. Identification of the document

Name:	Service policy of the Time-Stamping Authority (TSA)
Version:	201021
Description:	Service policy for the Qualified Time-Stamping Service of the Time-Stamping Authority of Firmaprofesional (TSA)
Date of Issue:	21/10/2020
OIDs:	0.4.0.2023.1.1
Location:	http://www.firmaprofesional.com/cps

2. Summary

Time-stamping is an on-line mechanism which demonstrates that a series of data has existed and has not been altered since a specific point in time.

Firmaprofesional is a Time-Stamping Authority (TSA) which acts as a trusted third party, attesting to the existence of such electronic data at a specific date and time.

The time-stamping services are not public, the service must be previously contracted with Firmaprofesional. Time-stamping services are sold in the form of annual packages, these specify the maximum number of time-stamping requests that a customer can make annually.

Firmaprofesional offers two different Time-Stamping services:

- **Time-Stamping Service:** The client makes a request for a time-stamp, in accordance with regulation RFC 3161, to a URL of Firmaprofesional. In response they will receive digital evidence signed by the TSA of Firmaprofesional.
- **Time-Stamping Service with Custody of Evidence:** Firmaprofesional will store and guard a copy of each generated digital evidence and, if required, make it available to the client.

Firmaprofesional will not store copies of time-stamps issued unless the custodial time-stamp service has been previously contracted.

3. Definitions and abbreviations

3.1. Definitions

- **Trust Service Provider:** a natural or legal person issuing electronic certificates or providing other services related to electronic signatures.
- **Time-stamp:** a special type of electronic signature issued by a trusted service provider that guarantees the integrity of a document at a specific date and time.
- **Time-Stamping Authority:** a trusted entity that issues time-stamps.
- **Hardware Security Module:** a hardware module used to perform cryptographic functions and safely store keys.
- **Hash function:** an operation performed on a data set of any size which produces another data set of fixed size, regardless of the original size, and which has the property of being associated unequivocally to the initial data.
- **Certificate Revocation Lists :** a list of revoked or suspended certificates.

3.2. Abbreviations

TSA	Time-Stamping Authority
TSP	Depending on the context: • Trust Service Provider • Time-Stamp Protocol
TST	Time-Stamp Token
IETF	Internet Engineering Task Force
CEN	European Committee for Standardization
FIPS	Federal Information Processing Standards
CWA	CEN Workshop Agreement
RFC	Request For Comment
UTC	Coordinated Universal Time
CRL	Certificate Revocation List
HSM	Hardware Security Module

4. General Concepts

4.1. Time-Stamping Authority (TSA)

A Time-Stamping Authority (TSA) is a Trust Service Provider that provides confirmation of the pre-existence of certain electronic documents at a given time.

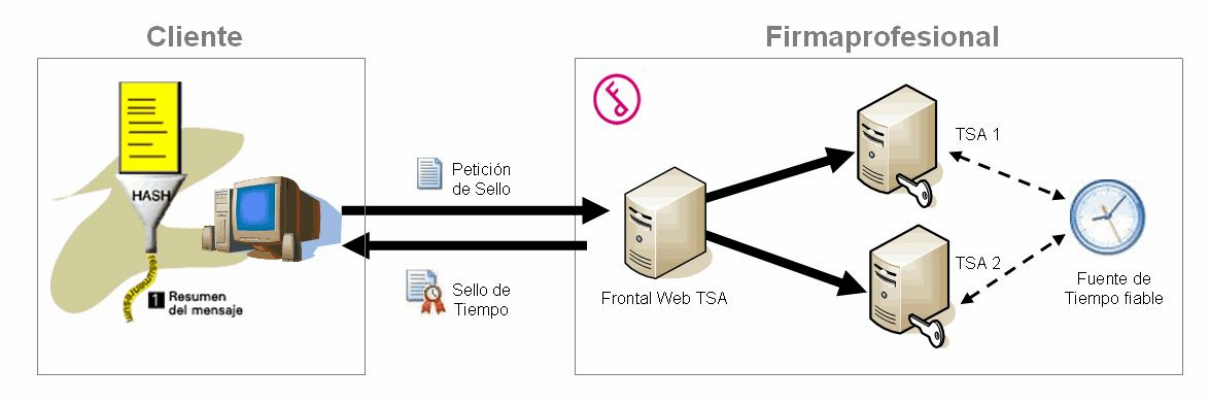
4.2. Time-Stamping Service

Time-stamping is an on-line mechanism which demonstrates that a series of data has existed and has not been altered since a specific point in time.

Firmaprofesional's Time-Stamping Service is based on the use of the TSP over HTTP, defined in regulation RFC 3161 "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".

The steps to generate a time-stamp are as follows:

- The client calculates the hash of the document to be sealed.
- The client sends a request for a time stamp to a URL specified by Firmaprofesional, following the RFC 3161 over HTTP protocol, including the hash of the document to be sealed.
- Firmaprofesional receives the request, carries out an access control of the client and checks if the request is complete and correct.
- If the result is correct, the TSA signs the petition and generates a time-stamp (including the hash of the document, the date and time obtained from a reliable source and the electronic signature of the TSA).
- The time-stamp is sent back to the client.
- The customer must validate the signature of the stamp and safeguard it appropriately.
- If the custodial service has been contracted, the TSA will keep a record of the responses generated, which will be available to the customer for future verification.



4.3. Clients

Clients must adapt their systems so that they can perform time-stamping requests using the TSPr protocol. Firmaprofesional does not provide any software nor integration libraries to the client to perform these functions.

There exist public libraries that implement the TSP protocol in various programming languages:

- **BouncyCastle** (http://www.bouncycastle.org): Set of cryptography libraries for implementing the TSP protocol in Java and C #.
- **OpenSSL** (http://www.openssl.org): The cryptography library OpenSSL implements the TSP protocol in C.
- **IAIK:** Java includes cryptography libraries that implement the TSP protocol. These libraries are free for non-commercial uses.
- **Adobe Reader:** The Adobe Reader application permits the validation of time-stamps included in PDF documents.
- **Prosign:** The PDF signing tool, offered for free by Firmaprofesional, permits the addition of time-stamps to the signed documents.

5. Participating Entities

5.1. Trust Service Providers (TSP)

According to Regulation (EU) 910/2014 a Trust Service Provider (TSP) is a natural or legal person who provides one or more trust services, either in a qualified or unqualified role.

The term Qualified Trust Service Provider refers to the Trust Service Provider that provides one or more qualified trust services and has been awarded the qualification by the supervisory body.

Firmaprofesional has been included in the Spanish TSL as a qualified provider since the entry into force of the European Regulation on 1 July 2016.

5.2. Time-Stamping Authority (TSA)

Firmaprofesional is a TSP that acts as a Time-Stamping Authority (TSA). Firmaprofesional offers trust services by its own means, without delegating to any other entity.

Firmaprofesional can use different systems to generate time-stamps, providing high availability for the service.

5.3. Client

Clients are users of the service, who send stamping requests and receive time-stamps following the protocol "RFC3161 Time-Stamp Protocol (TSP)".

The Time-Stamping services of Firmaprofesional are not public. To access the Time-Stamping services the client must previously contract them with Firmaprofesional.

5.3. Parties Relying on the Time-Stamps

The Regulation (EU) 910/2014, compiles and regulates the issue of time-stamps, defining them as "data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time".

Therefore, any user can freely validate time-stamps relying on the trust in Firmaprofesional as a Provider of Qualified Certification Services that issues qualified certificates.

6. Obligations and responsibilities

6.1. Firmaprofesional

6.1.1. Obligations

Firmaprofesional, in its capacity as a Time-Stamping Authority (TSA) is obliged to:

- Respect the provisions of this Time-Stamping Policy.
- Securely protect the private keys.
- Issue time-stamps in accordance with this Policy and the applicable standards.
- Ensure that the time and date included in the seals is within the margins of accuracy specified in the contract between the client and Firmaprofesional, which in no case may exceed one second[1].
- To issue time-stamps, free of data entry errors, according to the information provided by the client.
- To issue time-stamps whose minimum content, when applicable, is defined by the current regulations.
- To publish the Time-Stamping Policy.
- To inform clients and relying parties about any Policy modifications.
- To establish the mechanisms for the generation of relevant information on the described activities, protecting them against loss, destruction or falsification.
- To safeguard the issued time-stamps for those clients who have contracted the custodial service.

[1] ETSI EN 319 421 V1.1.1 Ap 7.7.2.b; ETSI 102 023 v010201 5.1; ETSI 101 861 v010201 5.2.1

Firmaprofesional, in its capacity as a Trust Service Provider, is liable for any breach of the provisions set out in this Time-Stamping Policy and, where applicable, for those set out in Law 59/2003, of 19 December, on electronic signatures or its implementation regulations.

Notwithstanding the foregoing, Firmaprofesional does not guarantee the algorithms or cryptographic standards employed nor accept liability for damage due to external attacks, provided that at all times due diligence has been applied according to the state of the art, and that they have acted in accordance with the provisions of the present TSA Policy and, where applicable, current legislation.

6.1.2. Obligations for the issue of qualified time-stamps

When Firmaprofesional certifies a time-stamp as qualified according to EU regulation No. 910/2014 (eIDAS), the public key certificate for signature verification is issued under the certificate policy set out in ETSI EN 319 411-2, which also incorporates the requirements of ETSI EN 319 411-1.

To indicate that the time-stamps are qualified, Firmaprofesional incorporates the field "Time-stamp policy" according to the Best practices Time-Stamp Policy (BTSP) with OID: 0.4.0.2023.1.1 as defined in the standard ETSI EN 319 421.

Firmaprofesional issues the qualified electronic stamps by means of a TSU exclusively for this purpose. For non-qualified stamps another TSU is available.[2]

6.1.3. Financial Responsibility

Firmaprofesional will be liable for damages, caused deliberately or by negligence, to any natural or legal person due to a breach of the obligations set out in EU Regulation[3] No 910/2014 of the European Parliament and of the Council of 23 July 2014.

6.1.4. Disclaimer

Firmaprofesional will not be liable for any of the following or under any of the following circumstances:

[2] In accordance with ETSI EN 319 421 v1.1.1 Ap 8.2

[3] In accordance with article 13 of Regulation ReIDAS.

- State of war, natural disasters, malfunction of electrical services, telecommunications and/or telephone networks or computer equipment used by the Customer or by third parties, or any other force majeure.
- Improper or fraudulent use of time-stamps.
- Misuse of the information contained in the Certificate or the CRL.
- For the content of messages or stamped documents.
- In relation to actions or omissions of the client.
    - Negligence in the safekeeping of access data to the time-stamping service, in ensuring its confidentiality and in the protection of all access or disclosure.
    - Excessive use of the time-stamp, in accordance with current legislation and this Policy TSA.
- In relation to acts or omissions of the User or party relying on the certificate.
    - Failure to check for the suspension or loss of validity of the electronic certificate of the TSA as published in the consultation service on the validity of the certificates or failure to verify the electronic signature.
- By the actions of persons, entities or organizations that, without having signed a contract with Firmaprofesional proceed to perform these services for third parties. Notwithstanding the above, the right to bring any legal actions that may apply will be reserved.

6.1.5. Cessation of the TSA activity

Before the cessation of its activity the TSA will perform the following actions:

- It will inform all subscribers, users or entities with which it has agreements or other type of relationship of the cessation with not less than 2 months notice or the period established by current legislation.
- It will revoke all authorization to outsourced entities to act on behalf of the TSA in the procedure for issuing time-stamps.

- It will inform the competent authorities, with the indicated advance period, of the cessation of its activity and the future of any time-stamps issued up to that date, specifying, where appropriate, if the management will be transferred and to whom.
- It will revoke the certificates of the TSU.[4]

6.2. Client

The Client is obliged to act in accordance with the regulations and also to:

- Respect the provisions of the contractual documents signed with the TSA.
- Verify the correctness of the digital signature of the time-stamp and validity of the certificate of the TSA at the time of signing.
- Verify that the hash contained in the time-stamp matches that which has been sent.
- Store and preserve time-stamps provided by the TSA. The Client is responsible for storing time-stamps, if it is anticipated that they will be needed in the future.

6.3. Party relying on the time-stamps

The Customer is obliged to comply with the provisions of the current regulations and also to:

- Verify the correctness of the signature of the time-stamp and the validity of the certificate of the TSA at the time of signing.

[4] In accordance with ETSI EN 319 421 v1.1.1 AP 7.14

7. Operational Requirements

7.1. Access control

Firmaprofesional will monitor access to the service based on IP addresses, hence the customer must inform Firmaprofesional of the IP addresses from which the requests will be made.

Alternatively it offers access control based on user name and password for environments with dynamic IP addresses.

7.2. Obtaining reliable time

As a reliable time source, Firmaprofesional has a Rubidium Atomic Clock, model **SyncServer 600**, with a precision, guaranteed by the manufacturer, of less than 1 microsecond per day lag accuracy. The atomic clock is synchronized by GPS, allowing a confidence level of Stratum 1. Synchronization with the ROA (see below) is also carried out over the internet following the NTP Protocol (RFC 1305 Network Time Protocol).

The main mission of the **Sección de Hora** (Time Section) of the **Real Instituto y Observatorio de la Armada en San Fernando** (**ROA**, Royal Institute and Observatory of the Navy in San Fernando) is to maintain the basic unit of time, which is declared for legal purposes as the National Standard of the unit, it also deals with maintenance and official dissemination of the standard "Coordinated Universal Time" (UTC), considered for all purposes as the basis of the legal time throughout the national territory (R.D. October 23, 1992, no. 1308/1992, declaring the Laboratory of the Royal Institute and Observatory of the Navy as the depository laboratory of the National Time Standard and laboratory associated with the Spanish Metrology Center). To achieve this there is a collaboration with the Consejo Superior de Investigaciones Científicas (CSIC, Higher Council for Scientific Research), to control and monitor the synchronization of the main time distribution machines in Spain, three of which belong to the Sección de Hora (two located in the INSOB and a third in Madrid).

7.3. Period of Custody

In the case of the Non-Custodial Time-Stamping Service the custody of the emitted replies is not guaranteed. Their adequate safe-keeping is the responsibility of the client.

7.4. Request for time-stamps

The applications for Time-Stamps must adhere to the syntax of Section 3.4. "Time-Stamp Protocol via http" of the standard "**RFC 3161 Time-Stamp Protocol (TSP)**", subject to the restrictions of standard ETSI TS 101 861.

The URL of the Time-Stamping without Custody service of Firmaprofesional is:

http://servicios.firmaprofesional.com/tsa

The URL of the Time-Stamping with Custody service of Firmaprofesional is:

http://servicios.firmaprofesional.com/tsadb

7.5. HASH Functions

The service supports the following hash algorithms in the requests. GOST3411, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, RIPEMD128, RIPEMD160, RIPEMD256.

It is recommended not to use the SHA-1 algorithm because it is considered unsafe. The CCN-CERT 807 guidelines, of January 2017, recommend the use of the SHA-256, SHA-384 and SHA-512 algorithms.

In the responses of the time-stamps the SHA-256 algorithm is used.

7.6. Format of the applications

The format for sending requests adheres to the following scheme:

Content type: application/timestamp-query

Method: POST

Content-length: ***required***

<<Contains the application for the Time-Stamp in ASN.1, coded in DER>>

Optional fields, according to the RFC 3161 specification, are treated as follows:

Field	Value
nonce	Optional. If present the response contains the same value.
reqPolicy	Not used
certReq	Not used
extensions	Not used

7.7. Format of the responses

If the application cannot be processed, an HTTP response is returned providing an error code when it is not possible to respond with a time-stamp. Possible errors are:

Cause	Error	Description
Missing content-length field	411	CONTENT_LENGTH REQUIRED
Content-length too large	413	REQUEST ENTITY TOO LARGE
Content-type incorrect	415	UNSUPPORTED MEDIA TYPE
The data is not a time-stamp request	400	BAD REQUEST
Server not responding	500	SERVER INTERNAL ERROR

If a browser or the GET method is used to access the URL of the service, the server will display a web page indicating the error (and will return a Code 200).

Responses are sent in the following format:

Content type: application/timestamp-reply

Method: **POST**

Content-length: **required**

<<Contains the application for the Time-Stamp in ASN.1, coded in DER >>

Optional fields, according to the RFC 3161 specification, are treated as follows:

Field	Value
Time-stamp policy	0.4.0.2023.1.1
ordering	False
nonce	If the request contains this the same value is returned. If not a new one is created.
Attached Certificates	<Certificate of the TSA>

	<Certificate of the Subordinate CA>
accuracy	Not present
tsa	Not present
extensions	Not present

7.8. Calibration loss control

Firmaprofesional has the correct calibration of its TSU clock under constant surveillance. In case of detecting a deviation greater than the one established in this policy, the TSA service will automatically stop.

7.9. Certificate of the TSA

7.9.1. Generation of the certificate

For the generation of the certificate of the Time-Stamping Authority, the **Secure Service Certification Policy** of Firmaprofesional (OID 1.3.6.1.4.1.13177.10.1.4.1) must be followed. It is available at http://www.firmaprofesional.com/cps.

The private keys[5] of the TSA are generated and safeguarded in a Hardware Security Module (HSM) that meets the requirements detailed in FIPS 140-2 Level 2 or higher, or with a level EAL 4+ or higher in accordance with ISO/IEC 15408.

Firmaprofesional has access to various TSA to ensure high availability for the time-stamping service.

The TSA certificates employed will have a minimum length of 2048 bits, a duration of 6 years and, as established in this policy, a duration for the keys of 3 years from the moment the associated certificate becomes valid.

When using time-stamps for procedures of a high-level of the National Security Scheme the instructions of the security standard CCN-STIC-807 must be followed.

[5] In accordance with ETSI EN 319 421 v1.1.1 Ap 7.6.2

7.9.2. Publication of the certificate

The certificate of the TSA is attached to the response of each Time-stamp issued. The certificate of the TSA Qualified service is published in: http://crl.firmaprofesional.com/tsa/tsa.crt

7.9.3. Change of the TSA certificate

Controls are in place to ensure the renewal of the keys before the expiry of their validity.

The TSA certificate can be changed at any time by another equally valid TSA certificate according to the **Secure Service Certification Policy** of Firmaprofesional.

This change will not be communicated to the service users, who must rely on all the stamps issued by Firmaprofesional and signed with valid TSA certificates within the certification hierarchy.

The associated keys will be destroyed in such a manner that they cannot be recovered, in accordance with the instructions of the manufacturer of the HSM that generates and stores them.

7.9.4. TSA Certificate in Production

The TSA certificate used in production has the following values:

Field	Value
Subject	CN = FIRMAPROFESIONAL CLOUD QUALIFIED TSU - 2020 organizationIdentifier = VATES-A62634068 O = Firmaprofesional S.A. C = ES
Issuer	CN = AC Firmaprofesional - CUALIFICADOS SERIALNUMBER = A62634068 OU = Certificados Cualificados O = Firmaprofesional S.A. C = ES
S/N	487cc77aacc40a8c693f98d4f217071d
Validity	notBefore: 06 agosto2020 12:39:33 notAfter: 05 agosto2026 12:39:33
Private Key Usage Period	3 años
Hash SHA1	0DE5286CD35DF67528E6E6FFAC3A380996C8F419

The TSA certificate previously used in production has the following values:

Field	Value
Subject	CN = FIRMAPROFESIONAL CLOUD QUALIFIED TSU organizationIdentifier = VATES-A62634068 O = Firmaprofesional S.A. C = ES
Issuer	CN = AC Firmaprofesional - INFRAESTRUCTURA SERIALNUMBER = A62634068 OU = Security Services O = Firmaprofesional S.A. C = ES
S/N	71 8d 3d 05 8e 49 40 29 5d 5a a0 22 df 53 08 55
Validity	notBefore: 06 febrero 2020 10:39:13 notAfter: 04 febrero 2026 10:39:13
Private Key Usage Period	3 años
Hash SHA1	4a f1 30 53 81 ea 97 04 59 c7 b9 16 c0 e2 35 1b 88 30 52 1e

Field	Value
Subject	CN = FIRMAPROFESIONAL CLOUD QUALIFIED TSU organizationIdentifier = VATES-A62634068 O = Firmaprofesional S.A. C = ES
Issuer	CN = AC Firmaprofesional - INFRAESTRUCTURA SERIALNUMBER = A62634068 OU = Security Services O = Firmaprofesional S.A. C = ES
S/N	55 81 05 6f d6 3c f7 b7
Validity	notBefore: Monday, 27 February 2017 14:19:33 notAfter: Sunday, 26 February 2023 14:19:33
Private Key Usage Period	3 years
Hash SHA1	cb 2c 8d 8c df f2 aa 58 00 6f b1 ea c5 71 a4 86 96 5c fe b2

firmaprofesional

Firmaprofesional, S.A.

October 2020