Disclosure Clauses for Qualified Time-Stamping Service

Document control

Formal status	Approved
Prepared by	Consorci AOC
Approved by	Executive Committee of the Consorci AOC on December 18, 2024
Date of creation	18/12/2024
Level of access to information	Public
Title	Disclosure Clauses for Qualified Time-Stamping Service
File	Clàusula de divulgació TSA1-1.0-EN.docx
Copy control	Only the copies available in the Consorci AOC's E-Office guarantee that the documents are up to date. Any copies printed or stored in different locations will be considered uncontrolled copies.
Copyright	This work is licensed under a Creative Commons Attribution-NonCommercial-No Derivative Works 3.0 Spain License. To view a copy, visit http://creativecommons.org/licenses/by-nc-sa/3.0/deed.ca or send a letter to Creative Commons, 171 Second Street, Suite 300, San Francisco, California 94105, USA.

Version control

Date:	18/11/2024
Description:	Initial version

Index

1. Full agreement

These disclosure clauses are an extract from the agreements established by the Declaration of Practices of the qualified time stamp (hereinafter **DP)** provided by the Consorci Administració Oberta de Catalunya (hereinafter, **Consorci AOC**), available in https://tsa.aoc.cat/regulacio/.

2. TSA Contact Information

The Consorci AOC Qualified Time Stamping Service Manager is responsible for the development, implementation and publication of the Consorci AOC Qualified Time Stamping DP, as well as relevant documents related to the provision of the Time Stamping Service. All queries and comments regarding the content of these documents can be addressed to:

Consorci Administració Oberta de Catalunya

Address:	C/ Salvador Espriu, 45.
CP:	08908
	L'Hospitales del Llobregat
Email:	suport@aoc.cat
Telephone:	(+34) 93 272 40 00

3. Types of certificates, and use of electronic time stamps

The TSU certificates of the Time Stamping Units (**TSUs***) operated by the* Time-Stamping Authority (**TSA)** are qualified certificates in accordance with Article and Annex III of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of ETSI EN 319 411-2 technical regulations, ETSI EN 319 412-3, ETSI EN 319 421 and ETSI EN 319 422.

With these qualified TSU certificates, the Consorci AOC offers under this document a type of time stamps:

- Qualified Time Stamps

This service has the policy identifier (OID) 0.4.0.2023.1.1, which corresponds to the BTSP (*Best practices Time-Stamp Policy*) defined in the ETSI EN 319 421 standard.

Electronic timestamps declared as qualified follow the indications of EU Regulation 910/2014 and the TSU certificate is issued under the policy declared in ETSI EN 319 411-2.

Our timestamps are issued in the format defined in the RFC 3161 standards and can be used for any purpose that requires guaranteeing the existence of a certain cryptographic summary at a given point in time.

The hashing algorithm used by the client in the request to represent the data to be sealed may be RIPEMD-160, SHA-1, SHA-256, SHA-384 or SHA-512. In accordance with the ETSI TS 119 312 standard and the CCN-STIC 807 Guide, it is recommended to use the SHA-256, SHA-384 or SHA-512 hashing algorithm.

The hashing algorithm used in signing the timestamp contained in the service response is SHA-256.

The Consorci AOC does not keep copies of the time stamps it issues. These will be valid until the expiry date of the certificate's certificate.

Customers who receive time stamping services must carry out the validation operations as provided for in **clause 8** and take into account the limitations and exclusions of **clause 9.**

4. Time synchronization

The declared time accuracy on time stamps with UTC time is 1 second with respect to official UTC time.

See section 2.8 of the Qualified Time Stamping DP for more information.

5. TSA Obligations

The Consorci AOC, acting as TSA, has the following obligations in the time stamping services it provides:

a) Provide services and issue time stamps in accordance with the DP.
b) All those that derive from the content of this document, from the documents "Declaration of Certification Practices (DPC) Consorci AOC Certification Authority" and "Certification Policy for Consorci AOC Devices and Infrastructures" that is applicable (see point 1.1), as well as from current legislation.

See point 1.4.1 of the DP for Qualified Time Stamping for more information.

6. Obligations of subscribers

The obligations of the Subscriber of a time stamping service under this DP are:

a) Use the service in accordance with the DP.
b) Diligently guard the secret keys, passwords or pins used for the identification and authentication of the Subscriber to the service, taking reasonable precautions to prevent their loss, disclosure, modification or unauthorized use.
c) Validate the time stamps contained in the service's responses at the time of receipt of the responses in accordance with the provisions of **clause 8**.
d) Immediately inform the TSA of any incident or event that affects the service provided or that may affect the validity of the time stamps.

e) Use the Service in accordance with the Law and the limitations set out in **clause 9** of this Disclosure Clause and in the General Conditions of Provision of the AOC Services published at: https://web.aoc.cat/blog/serveis/condicions-prestacio-serveis-aoc/

See section 1.4.3 of the DP for Qualified Time Stamping for more information.

7. Obligations of the Trusting Third Party

The obligations of the relying Party (also referred to as "the User Parties") on a timestamp issued by a timestamping service under this RFP are:

a) Validate the timestamp as specified in **clause 8**, at the current time or, where applicable, at the time when the integrity of the timestamp has been protected (e.g. by means of an additional timestamp, or by storing the timestamp securely).

   • As a verifier, if the 'Relying Third Party' relies on an electronic signature corresponding to an unverified electronic timestamp, they will assume all the risks and consequences of this action.

b) Take into account the limitations of use specified in **clause 9**.

   • To make correct use of the status information of electronic time stamps and not to compromise the security of the Consorci AOC's public time stamping services.

See Section 1.4.4 of the DP for Qualified Time Stamping for more information.

8. Validating the time stamp

The validation of a time stamp must be carried out by the interested party by their own means, using the stamped data and the certificate of the TSU with the private key of which the time stamp has been signed.

The certificates of the Consorci AOC's TSUs, both the current ones, in active status, and the previous ones, in the deactivated or finished state, are published on the website https://tsa.aoc.cat/regulacio/ .

To validate a timestamp at a certain time, the following verifications must be carried out:

   • The hash of the data contained in the timestamp is equal to the hash of the stamped data.
   • The digital signature of the time stamp is correct.
   • The TSU private key used has not been compromised prior to the time of timestamp validation.
   • The hashing algorithms used (in the hash of the stamped data and in the timestamp signature), and the algorithm and key size of the timestamp signature can continue to be considered secure at the time of timestamp validation.
      • In the case of the time-rated stamping service, verify that the TSU certificate has been issued by a Certification Authority (**CA**) of the Consorci AOC whose certificate is included in the Spanish Trust-service Status List (**TSL),** *in a time-rated time-stamping service in granted status* at the time of validation of the time stamp or at the time of issue of the time stamp.

The Catalan Public Administrations will be able to carry out these verifications using the Validator Service offered by the Consorci AOC itself.

9. Limitation and exclusion of liability

The Consorci AOC will respond to the corresponding functions in accordance with the DP Qualified Time Stamp, taking into account the following limitations and exclusions of liability:

- Time stamping services under this DP do not store or guard issued time stamps, but Consorci AOC will maintain audit records of requests and responses for a minimum period of 15 years, for the qualified time stamping service, from the expiration of the active service certificate at the time of operation or from the end of the service, so that the timestamps issued can be identified.
- The Consorci AOC does not offer any software, library or service to make requests to time stamping services or to process their responses, and it is the responsibility of the Subscriber or its end users to adapt their systems or use existing software on the market to make the requests and process the responses. Therefore, Consorci AOC will not be responsible for the correct functioning of the applications used by the Subscriber for this purpose, nor for deterioration or breakdowns in the equipment, data or installation necessary to run the service for reasons not directly attributable to the use of the service.
- Consorci AOC will not be liable for damages arising from or related to the non-performance or defective performance of the obligations borne by the Subscriber, nor for the incorrect use of the services and the associated keys for their use, nor for any indirect damage that may result from the use of the service, in particular, loss of profit, loss of income or loss of data, not giving rise to any type of right to compensation.
- The Consorci AOC shall not assume any liability for the non-performance or delay in the performance of any of the obligations under this contract if such failure to perform or delay results from or is the consequence of force majeure, unforeseeable circumstances or, in general, any circumstance over which the Consorci AOC cannot reasonably control.
- In particular, the Consorci AOC will not be able to assume any responsibility for the data or content on which an electronic time stamp is applied.

10. Applicable agreements and declaration of internships

The Consorci AOC's Time Stamping Service is technically and operationally regulated by the Qualified Time Stamping DP, by its subsequent actions, as well as by the complementary documentation.

Such time-stamping DP as well as the integration documentation can be consulted at: https://tsa.aoc.cat/regulacio/

The General Conditions for the provision of AOC Services published at: https://web.aoc.cat/blog/serveis/condicions-prestacio-serveis-aoc/

In all matters not provided for in this Disclosure Clause, the provisions of the DP on time stamping will apply. However, in the event of a contradiction between the terms of this document and the DP of time stamping, the latter will prevail in any case.

11. Privacy Policy

The Consorci AOC's Time Stamping Service does not identify its users, nor do the operations it carries out process personal data.

12. Refund Policy

Not applicable.

13. Applicable Law, Claims and Dispute Resolution

13.1. Applicable

The parties will be governed by Spanish law, in particular by Law 6/2020, of 11 November, regulating certain aspects of electronic trust services and 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.

13.2. Out-of-court dispute resolution

The Consorci AOC establishes, in its legal instruments with subscribers and verifiers, the applicable mediation and conflict resolution procedures, for which purpose, its consideration as a Public Administration is taken into account.

Situations of discrepancy arising from the use of the time stamping services issued by the Consorci AOC are resolved by applying the same criteria of competence as in the case of documents signed in writing.

13.3. Competent jurisdiction

The Time Stamping Authority establishes, in its binding legal instruments with subscribers and verifiers, a competent jurisdiction clause, which indicates that international judicial jurisdiction corresponds to Spanish judges. Territorial and functional jurisdiction is determined by virtue of the rules of private international law and rules of procedural law that are applicable. Likewise, the applicable administrative legislation is taken into account.

14.TSA and License Depository, Trust Marks, and Auditing

Consorci AOC is a Qualified Trust Service Provider, in application of EU Regulation No. 910/2014 (eIDAS), having passed the conformity assessments applicable to the Service subject to this document.