Administració Oberta de Catalunya

Practices Statement of the Time Stamping Service

Generalitat de Catalunya

Localret

Administració Oberta de Catalunya

Document control

Formal status	Approved
Prepared by	Consorci AOC
Approved by	Executive Committe of the Consorci AOC on December 18, 2024
Date of creation	18/12/2024
Level of access to information	Public
Title	Practices Statement of the Time Stamping Service
File	DP_TSA-2.0-EN.docx
Copy control	Only the copies available in the Consorci AOC's E-Office guarantee the updating of the documents. Any copies printed or stored in different locations will be considered uncontrolled copies.
Copyright	

Version control

Version	Description	Date
1.0	Initial version	18/12/2024
2.0	Non qualified service incorporation	17/12/2025

Administració Oberta de Catalunya

Table of Contents

Administració Oberta de Catalunya

1. Introduction

1.1. Overview

This document constitutes the Practices Statement (hereinafter, **DP)** of the following services for the issuance of electronic time stamps (hereinafter, time stamping services) provided by the Consorci Administració Oberta de Catalunya (hereinafter, Consorci AOC):

- **SERVICE FOR THE ISSUANCE OF QUALIFIED ELECTRONIC TIME STAMPS** (hereinafter, qualified time stamping service)
- **SERVICE FOR THE ISSUANCE OF NON QUALIFIED ELECTRONIC TIME STAMPS** (hereinafter, non-qualified time stamping service)

The provision of these services is carried out in accordance with 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, as amended by Regulation (EU) 2024/1183, of 11 April 2024 (hereinafter, eIDAS Regulation) and Law 6/2020, of 11 November, regulating certain aspects of electronic trust services (hereinafter, Law 6/2020).

As not specified in this document, time stamping services under this DP are governed by what is specified in the documents "Consorci AOC Certification Authority Certification Practice Statement (CPP), "Consorci AOC Certification Policy for Devices and Infrastructures" and "Description of Consorci AOC Certificate Profiles" published on the https://epscd.aoc.cat/ca/index.html#politiques https://epscd.aoc.cat/ca/index.htmlwebsite, in so far as it is not applicable exclusively to the certificate issuance services of the Consorci AOC, and in so far as it is applicable to the certificates of the Consorci AOC's time stamping services (see OID certificate policies in point 1.2).

To provide the services for the issuance of electronic time stamps, the Consorci AOC subcontracts to a third-party provider (hereinafter referred to as the technology provider) the hosting, management and operation of the time stamping services under this DP.

Time stamping services under this DP allow you to obtain a reliable and secure timestamp with all the guarantees, both legal and technical, established by current regulations. These services make it possible to accredit, by means of the timestamp reported by the service, the existence of an element in electronic format (document, signature, etc.) at a given moment in time. Among the advantages of these services are:

- Security: The timestamp is a secure and reliable way to obtain timestamps while also linking them to a document. The date and time of the time stamp is protected by robust security mechanisms (digital signature).
- Trusted third party: each time stamp that is issued is guaranteed by a trusted third party, in this case the Consorci AOC and CATCert.
- Electronic evidence: each time stamp is electronic evidence that accredits a time point in time in which the existence of a document can be assured.
- Savings: the Consorci AOC assumes the cost of the service and offers it free of charge for Catalan public sector applications.

The timestamps issued under this DP are in accordance with the BTSP Policy (Best practices Time-Stamp Policy) defined in the European standard ETSI EN 319 421, identified by OID 0.4.0.2023.1.1.

Timestamps issued under this DP include the BTSP Policy OID 0.4.0.2023.1.1.

The accuracy of the timestamps issued under this DP will be 1 second with respect to UTC time.

The requests, responses and certificates of the time stamping services under this DP are in accordance with the European standard ETSI EN 319 422.

1.2. Name of the document and identification

This document has the following identification data:

Name	Consorci AOC Time Stamping Service Practice Statement
Version	2.0
OID Qualified Time Stamping Service Practice Statement	1.3.6.1.4.1.15096.3.2
OID Qualified Time Stamping Service Policy	0.4.0.2023.1.1 (ETSI EN 319 421 BTSP)
OID Non-Qualified Time Stamping Service Policy	0.4.0.2023.1.1 (ETSI EN 319 421 BTSP)
OID Qualified Time Stamping Service Certificate Policies (TSU Certificates)	1.3.6.1.4.1.15096.1.3.2.112 (Consorci AOC) 0.4.0.194112.1.1 (ETSI EN 319 411-2 QCP-l)
OID Non-Qualified Time Stamping Service Certificate Policies (TSU Certificates)	1.3.6.1.4.1.15096.1.3.2.113 (Consorci AOC)
Localization	https://www.tsa.aoc.cat/regulacio

1.3. Participants

1.3.1. Time Stamping Authority (TSA)

A Time-Stamping Authority (TSA) is a Trusted Service Provider that provides time-stamping services. The role of a TSA is to become a trusted third party by certifying the existence of the stamped data on a specific date and time.

A TSA operates one or more Time-Stamping Units (TSUs) for each of the time-stamping services it provides.

The TSA shall be responsible for the provision of the time stamping services under this RFP, and for the fulfillment of its obligations and the obligations of all external organizations used to provide part of these services.

The Consorci AOC acts as a TSA under this DP.

1.3.2. Subscriber

It is an entity of the Public Sector of Catalonia that requests the use of a time stamping service under this DP, to which time stamps are issued.

It will include both the Subscriber's own applications and the individuals (end users) who depend on it and who may make requests for time stamps to the TSA using their own resources and means, who assume the fulfillment of some of the Subscriber's obligations, without prejudice to the Subscriber's liability, in the event of non-compliance with these obligations.

1.3.3. Third party who trusts

It is the natural person or entity (with or without legal personality) that receives an electronic transaction with a time stamp issued by a time stamping service under this DP, and who voluntarily relies on this time stamp (Relying party).

1.4. Obligations of participants

1.4.1. TSA Obligations

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

- Provide the services and issue the time stamps in accordance with this DP.
- Keep the documentation specified in point 1.5.5 published.
- Modify this document and notify, where appropriate, the modifications in accordance with the provisions of point 1.5.6.
- Keep the certificates associated with the private keys used to sign the timestamps (TSU certificates) published.
- All those that derive from the content of the documents " Certification Practices Statement (DPC) Consorci AOC Certification Authority " and " Consorci AOC Certification Policy for Devices and Infrastructures" that are applicable (see point 1.1), as well as from current legislation.

1.4.2. Obligations of external organizations providing part of the services

The Consorci AOC, for the hosting, management and operation and monitoring of the time stamping services it provides under this DP, uses the services of external organizations that are subject to the following obligations:

- Management and operation (the technology provider)
    - Comply with the agreements of the contracts signed with the Consorci AOC.
    - To control and supervise the operation of the services to ensure that they are provided in accordance with this DP.
    - Install, configure, maintain, operate and consult audit logs of the hardware and software elements of the services.

- Establish the necessary security measures and controls to protect the system and the private keys of the services.
- To carry out the services using the appropriate technical and material means, as well as the qualified personnel required by the applicable standards.
- To comply with the quality levels of the services required by the applicable standards, in terms of technical, operational and security aspects.
- Guarantee that the time stamps issued are faithful to the information in the corresponding requests.
- Guarantee the date and time of the timestamps issued with an accuracy of 1 second with respect to UTC time.
- Store and safeguard the audit logs of the hardware and software elements of the services, in the case of requests and responses, for the minimum period established in point 2.10.
- Comply with Service Level Agreements (SLAs) for availability, infrastructure monitoring and 24x7 incident support.
- All those derived from current legislation.

- Data Processing Centers (DPCs)
  - Comply with the agreements of the contracts signed with the technology provider.
  - Prohibit access to the service area to any third party other than the data centre staff or authorized by the technology provider and maintain at all times a register of the persons authorized by the technology provider who access the Service Area.
  - Comply with the instructions given by the technology provider and agreed with the DPC regarding the handling of their equipment.
  - Not have any control over the information of the services transmitted through the facilities, nor examine the use that customers of the services make of the data, nor know the type of information they send, receive or store.
  - Comply with availability SLAs, infrastructure monitoring and 24x7 incident support.
  - All those derived from current legislation.
- Cloud computing
  - Comply with the agreements of the contracts signed with the technology provider.
  - Location of servers in the European Union.
  - Two-factor authentication for service administrators with password policy.
  - Access control defined for each application and user type.
  - Comply with availability SLAs, infrastructure monitoring and 24x7 incident support.
  - All those derived from current legislation.

1.4.3. Obligations of the Subscriber

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

- Comply with the provisions of the General Conditions for the Provision of Services of the Consorci AOC and the Disclosure Clauses of the time stamping service.

- Use the service in accordance with this DP.
- 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.
- Adapt its information systems to the requirements set out in the technical integration documentation to make requests to the service, in accordance with the provisions of point 2.5, and to process its responses, in accordance with the provisions of point 2.6.
- Validate the time stamps contained in the service responses in accordance with the provisions of point 2.7, at the time of receipt of the responses.
- Immediately inform the TSA of any incident or event that affects the service provided or that may affect the validity of the time stamps.
- Take into account the limitations of use specified in point 1.7.
- To duly inform end users of the above obligations.
- Designate a person in charge of the entity, and a technical manager for each of the applications under the affiliation of the entity that act as consumers of the service.

1.4.4. Obligations of the Trusting Third Party

The obligations of the Third Party relying on a timestamp issued by a timestamping service under this RFP are:

- Validate the time stamp in accordance with the one specified in point 2.7, at the current time or, if applicable, at the time when the integrity of the time stamp has been protected (for example, by means of an additional time stamp, or by storing the time stamp securely).
- Take into account the limitations of use specified in point 1.7.

1.5. Document administration

1.5.1. Organization

The drafting, publication, revision and modification of this DP is the responsibility of:

Organization	Consorci Administració Oberta de Catalunya (Consorci AOC)
Email	suport@aoc.cat
Website	https://www.aoc.cat

1.5.2. Contact details

For any queries about this PD, you can contact:

Organization	Consorci Administració Oberta de Catalunya (Consorci AOC)
Responsible	Responsible for the Time Stamping Services of the Consorci AOC
Email	scd@aoc.cat
Telephone	+34 93 272 40 00 - 900 90 50 90

1.5.3. Responsible for determining the adequacy of the DP with the Policies

The Head of the Digital Certification Service of the Consorci AOC is responsible for determining the suitability of the DP with the Policies.

1.5.4. Approval procedure

The Consorci AOC's documentary and organisational system guarantees, through the existence and application of the corresponding procedures, the correct maintenance of the DP and the specifications of the procedure for the publication of service specifications.

The initial version of this DP is approved by the Executive Committee of the Consorci AOC, which is the collegiate body of executive management of the Consorci AOC. The managing director of the Consorci AOC is competent to approve successive modifications.

1.5.5. Published documentation

The Consorci AOC makes available to all interested parties, in the public repository https://tsa.aoc.cat/regulacio/, the following documentation of the time stamping services under this DP:

- This DP.
- Disclosure Clauses.

The Consorci AOC publishes, once approved and in force, any new version of this documentation, keeping all its previous versions published.

1.5.6. Modifications

This document will be modified when there are significant changes in the provision of the services subject to it or when revisions to the document are made. There will be at least one biennial review of the document, in the event that there are no significant changes in the provision of services beforehand. Changes and revisions will be reflected in the version control panel at the beginning of the document.

Modifications to this document will be notified to the Subscribers and the Third Parties they entrust, when the changes in the provision of the services directly affect their rights and obligations, in accordance with the provisions of the Disclosure Clauses of the services. Notification of modifications may be published by the Consorci AOC in the public repository https://tsa.aoc.cat/regulacio/.

1.6. Responsibility

The Consorci AOC will be liable for damages caused deliberately or by negligence to any natural person or entity (with or without legal personality) due to non-compliance with the obligations established in the eIDAS Regulation and Law 6/2020 regarding time stamping services under this DP.

This liability is limited by:

- Causes of out of majority.
- Improper use of the service.
- Due to non-compliance with the obligations of the Subscriber or the Third Party that relies established in this DP, as well as in the General Conditions of Service Provision of the Consorci AOC and the Service Disclosure Clauses.

1.7. Limitations of use

- The time stamps issued by the time stamping services under this DP are intended to be used within the scope of all Catalan Public Administrations, to guarantee the existence of electronic signatures and electronic stamps that are presented to the Catalan Public Administrations at a certain point in time, as well as to guarantee transactions and imputability in processes between citizens, companies and the administrations themselves.
- The timestamping services under this DP do not store or guard the timestamps issued, but they do store and safeguard audit logs of the requests and responses of the services that allow the identification of the timestamps issued.
- The Consorci AOC does not offer any software, library or service to make requests to time stamping services under this DP, as specified in point 2.5, nor to process their responses, as specified in point 2.6, 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.

2. Operational requirements

2.1. How the time stamping service works

The time stamping service uses the protocol defined in the RFC 3161 standard on HTTPS communication, in accordance with the European standard ETSI EN 319 422.

The steps of the protocol are:

- The client sends a timestamp request containing the hash of the data to be stamped to a specific URL of the service, according to the format established in the RFC 3161 standard.
- The service verifies the request and, if it is valid, issues the timestamp, for which it signs the hash of the data to be stamped together with the current date and time and other data with the private key associated with an active timestamp certificate of the service, according to the format established in the RFC 3161 standard.
- The timestamp is sent to the client synchronously in a response to the request, according to the format established in the RFC 3161 standard.

The customer is obliged to validate the time stamp issued by the service, in accordance with the provisions of point 2.7.

2.2. Private keys and timestamp certificates

The private keys used for the signing of time stamps (time stamp private keys or TSU private keys) are generated and stored in a secure cryptographic device (HSM) with Common Criteria EAL 4 or higher certification, FIPS 140-3 Level 3 or higher.

The certificates associated with the private keys used for the signing of the time stamps (time stamp certificates or TSU certificates) are electronic stamp certificates issued by the Consorci AOC under the certificate policies of the time stamping service (see OID in point 1.2), in accordance with the European standard ETSI EN 319 422, and in accordance with the documents " Certification Practices Statement (DPC) Consorci AOC Certification Authority ", "Certification Policy for Consorci AOC Devices and Infrastructure" and "Description of Consorci AOC Certificate Profiles" published on the https://epscd.aoc.cat/ca/index.html#politiques website.

Qualified time stamp service certificates will be qualified according to European norm ETSI EN 319 411-2.

Time stamping certificates will have a validity period of 5 years in case of qualified certificates and 10 years for non-qualified. Private timestamp keys will have a validity period of 2 years for qualified certificates and 5 years for non-qualified. Before the end of the validity period of a private key, new keys will be generated and a new certificate will be issued that will replace the previous ones in the signing of the timestamps, thus guaranteeing a minimum validity of the timestamps of 3 years for qualified time stamp service and 5 years for non-qualified one, if there is no revocation of the certificate before its expiration.

After the validity period of a timestamp private key has expired and before the expiration of the associated certificate, the private key will be destroyed, including all its copies, in the following way that prevents its recovery:

- A secure erasure of the private key will be carried out on the cryptographic devices (HSMs) that have it stored, following the steps described in the HSM administration manual.

- A secure erasure of all backups of the private key will be performed.

A private key and a timestamp certificate can be in one of the following three states:

- Active: While the private key is being used to sign timestamps.
- Disabled: when the private key has ceased to be used for signing timestamps, before the end of its validity period.
- Finished: When the private key has been destroyed and the certificate has expired or has been revoked.

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

Digital certificates of qualified time stamp service TSU, with Policy OID 1.3.6.1.4.1.15096.1.3.2.112, are going to be:

- Subject: CN=CONSORCI AOC Q TSU 2024, organizationIdentifier=VATES-Q0801175A, O=CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA, C=ES

  Issuer: "SubCA Q TSA (G3) A.5”

  Algorithm and key lenght: RSA 2048

  Validity: 5 years. Until November 3, 2029.

  Private key usage period: 2 years. Until November 3, 2026.

- Subject: CN=CONSORCI AOC Q TSU 2025, organizationIdentifier=VATES-Q0801175A, O=CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA, C=ES
  Issuer: "SubCA Q TSA (G3) A.5”

  Algorithm and key lenght: RSA 3072

  Validity: 5 years. Until December 15, 2030.

  Private key usage period: 2 years. Until December 15, 2027.

For non-qualified time stamp service, with Policy OID 1.3.6.1.4.1.15096.1.3.2.113, TSU certificate will be:

Subject: CN=CONSORCI AOC TSU 2025, organizationIdentifier=VATES-Q0801175A, O=CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA, C=ES
Issuer: "SubCA TSAnoQ (G3) A.6”
Algorithm and key lenght: RSA 3072
Validity: 10 years. Until December 15, 2035
Private key usage period: 5 years. Until December 15, 2030

2.3. Time Stamping Unit (TSU)

A Time-Stamping Unit (TSU) is a set of hardware and software that is managed as a unit and has a single timestamp signing key active at an instant of time (private time-stamping key or TSU private key).

Time stamps are issued by TSUs for time stamping services provided by the TSA.

A time stamping service will only have one TSU active, except during the transitional period of replacing the keys and the service certificate (TSU replacement), during which the previous TSU, with the previous keys and the previous certificate, and the new TSU, with the new keys and the new certificate, may be active.

2.4. Access Control

Access control to the time stamping service by Subscribers is done by username and password.

2.5. Time stamp application

To make a timestamp request, the customer must send a request containing the hash of the data to be stamped to a specific URL of the timestamping service provided by the Consorci AOC.

The request will be sent over an authenticated HTTPS communication with username and password.

The request must use the syntax defined in the RFC 3161 standard, in accordance with the European standard ETSI EN 319 422.

2.6. Response format

The response of the time stamping service uses the syntax defined in the RFC 3161 standard, according to the European standard ETSI EN 319 422.

If there is no error, the response includes the timestamp issued, signed with the private key of the corresponding active TSU, which contains, among other data, the same hash value of the data to be stamped in the request and the current date and time of the TSU server processing the request.

The issued timestamp contains the BTSP Policy OID 0.4.0.2023.1.1.

In the case of the qualified time stamping service, the issued time stamp contains the extension qcStatements with the value specified in the European standard ETSI EN 319 422 for qualified time stamps.

In the event of any error, the response will include the corresponding error code defined in the RFC 3161 standard.

2.7. 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 TSU of the Consorci AOC, both the current ones, in active state, and the previous ones, in deactivated or finished state, are published on the https://tsa.aoc.cat/regulacio/ website.

To validate a timestamp at a given time, the following verifications must be performed:

- 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 to sign the timestamp has not been compromised prior to the time of timestamp validation. To perform this verification:

  During the validity period of the TSU certificate (before its expiry), its revocation status can be consulted through the OCSP or CRL service, in accordance with the procedures indicated in the document "Certification Practices Statement (DPC) Consorci AOC Certification Authority" published on the https://epscd.aoc.cat/ca/index.html#politiques website.

  - After the validity period of the TSU certificate (after its expiration), its revocation status can be checked only through the OCSP service, as the OCSP service returns the revoked status of the certificates after their expiration (the CRL does not keep the revoked certificates after their expiration), and the TSA can guarantee that the TSU private key has not been compromised after the expiration of the certificate of the TSU.
  - The Consorci AOC guarantees that the private keys of its TSU have not been compromised after the expiration of the respective TSU certificates by destroying the private keys before the expiration of the certificates.

- The hashing algorithms used in the timestamp (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-stamping service, 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 timestamp or at the time of issuance of the timestamp time, in accordance with the eIDAS Regulation and the European standard ETSI TS 119 612.

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

In the event of a security incident due to compromise or suspected compromise of the TSU private key used to sign the timestamp or due to loss of calibration of the clock of the server that issued the timestamp, the timestamp can be considered valid, if the TSA confirms that the timestamp has not been affected by the incident.

2.8. Time synchronization

A synchronization of the clock of the TSU servers with two UTC Stratum 1 time sources is performed using the NTP protocol (RFC 5905 Network Time Protocol Version 4), monitoring this synchronization at all times:

- Time Section of the Royal Institute and Observatory of the Navy in San Fernando (ROA)
- Time synchronization service of the Scientific Computer Center of Andalusia (CICA)

The declared time precision on time stamps with UTC time is 1 second. The TSU servers will not issue time stamps in case they detect a possible larger difference between their clocks and the UTC time sources with which they are synchronized.

2.9. Hashing algorithms

The hashing algorithm used by the client in the request to represent the data to be sealed can 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.

2.10. Audit logs

The TSA collects audit logs of the systems involved in generic and service-specific time stamping services.

Generic audit logs include, but are not limited to, events relating to:

- Access to safety zones
- Access to infrastructure systems
- Cryptographic operations

Audit logs specific to time stamping services include all events related to:

- Requests and answers.
- Life cycle of TSU keys and certificates.
- Synchronization and detection of loss of synchronization of the clock of the TSU servers with the UTC time sources.

The Consorci AOC will keep the audit records of requests and responses for a minimum period of 5 years for non-qualified time stamp service and 15 years, for the qualified time stamping service, from the expiration of the active service certificate at the time of the operation or from the end of the service.

2.11. Security incidents

The Consorci AOC's Disaster Recovery Plan contemplates cases of security incidents due to compromise or suspected compromise of the private key of a TSU and loss of calibration of the clock of a server of a TSU, which may have affected time stamps issued.

In the event of any of these security incidents, the Consorci AOC will provide Subscribers and Trusted Third Parties with information that can be used to identify timestamps that may have been affected.

2.12. Cessation of activity

The Consorci AOC has a Cessation Plan which establishes the actions to be carried out for the cessation of the activity of the time stamping services, including the revocation of all current certificates and the destruction of all private keys of the TSU of the services, both the current, in active state, and the previous ones, in the disabled state (the previous certificates in the finished

state are not valid, and the previous private keys in the finished state have already been destroyed).

The termination of the services will be communicated in advance to the Subscribers and all interested parties with whom the Consorci AOC has agreements or other types of relationships, in the case of the qualified time stamping service, with the minimum legally required notice.

3. Physical, procedural and personnel security controls

3.1. Physical security controls

The facilities that house the time stamping services infrastructure managed by the technology provider are subject to the annual validations of the UNE-ISO/IEC 27001 standard, which regulates the establishment of appropriate processes to guarantee correct security management in information systems.

3.1.1. Location and characteristics of the DPC

The infrastructure of the time stamping services managed by the technology provider is located in two data centers (DPCs) that guarantee the 24/7 availability of the communication systems and the availability of the service systems.

Data Centers are located within the territory of the European Union.

3.1.2. Physical Access Control

Data Processing Centers have the following physical security measures:

- Video surveillance and perimeter video recording at entrances, parking and facilities areas.
- 24x7 staff at the center.
- Access control to the building:
    - The DPC has an access control system that guarantees 24x7x365 secure access to the authorized personnel of the technology provider in the contracted service area.
    - Accesses are recorded individually with personal data of the authorized personnel of the technology provider.
    - Multi-level access is restricted to all sensitive areas of the school, with a contactless card, fingerprint and/or password.
    - Access to the security areas is protected with dual control and constantly monitored by CCTV and opening sensors in the area.

3.1.3. Power supply and air conditioning

The DPCs have high availability energy services with the following infrastructures:

- UPS rooms alternate with 120kvAs UPS in 2N configuration.
- Support generator sets in N+1 configuration.
- Fuel tanks for an autonomy of more than 48 hours of operation in the DPC.
- Room electrical panels powered by independent UPS groups.

The Technical Rooms are air-conditioned with split air condensation equipment, with air drive through false floors and humidifier of the environment, with redundant and independent direct expansion in each room, in N + 1 rotary configuration. The supply of outside air for ventilation of the CPD rooms is taken from the network of ducts from the outside air drive fan, which passes through a filtering unit that maintains biological conditions and active chemicals.

3.1.4. Exposure to water

The DPCs are located in an area where the risk of flooding is zero, being located 1500 meters from a type 5 risk area, low frequency (less than 500 years).

3.1.5. Fire protection and prevention

The fire extinguishing system of the DPCs covers technical rooms and critical facilities:

- Detection systems consisting of ionic smoke and flue gas detectors.
- Detection areas controlled by a modular micro-processed analogue control unit with full autonomy of signaling, fire centralization and breakdown.
- Fire extinguishing agent FE-13

3.1.6. Media storage

Each detachable storage medium (tapes, cartridges, CDs, discs, etc.) remains only within the reach of authorized personnel due to the physical access measures to the data center and the corresponding RACK cabinet.

3.1.7. Removal of information media

When it is no longer useful, sensitive information is destroyed in the most appropriate way for the medium that contains it:

- Printed matter and paper: by means of shredders or in bins arranged for this purpose for their subsequent controlled destruction.
- Storage media: Before being discarded or reused, they must be processed to ensure that the information contained in them has been securely disposed of.

3.1.8. Off-site backup

A backup copy will be kept on a different data center from which the service is provided with a frequency of less than 7 days.

3.2. Procedural controls

3.2.1. Trust roles

The following table indicates the trust roles of the time stamping services under this DP, as specified in the ETSI EN 319 401 standard:

ROLE OF TRUST	DESCRIPTION
Security Officers	General responsible for administering the application of security practices.
System Administrators	Authorized to install, configure and maintain the PSC's trusted systems for the management of services. This includes system recovery.
System Operators	Responsible for operating the TSP's trust systems on a day-to-day basis. Authorized to make system backups.
System Auditors	Authorized to view the files and audit logs of the TSP's trusted systems.

3.2.2. Number of people required per task

At least two people are required for the execution of tasks in each trust role classified as critical for time-stamping services under this PD, such as tasks related to cryptographic devices (HSMs) where the private keys of the services are generated and used.

3.2.3. Identification and authentication for each role

Each role is assigned one or more people, if applicable, designated by the management of the Consorci AOC or the technology provider.

Each person only controls the assets necessary for their role, thus ensuring that no one person accesses unassigned resources.

Access to resources is carried out, depending on the asset, through elements such as username and password, certificate, two-factor authentication, cards and/or passwords.

3.2.4. Roles that require separation of duties

The trusted role of Security Managers cannot be exercised by the same people who exercise any other role of trust.

3.3. Personnel controls

The personnel affected by the provisions of this section are those assigned to the roles of trust by the Consorci AOC and the technology provider.

3.3.1. Qualification, experience, and authorization requirements

The TSA ensures that the designated personnel are reliable and have the necessary qualifications and experience for the provision of the services offered and, in particular, that they have minimum knowledge of security and management. The foregoing is required without prejudice to the possibility that the TSA may supply the qualification and experience requirements through appropriate training and training.

3.3.2. Background Check Procedures

The TSA may request certificates proving the non-existence of a criminal record for its employees as long as the applicable regulation allows it.

3.3.3. Education Requirements

For new recruits, the area or service managers in question, in addition to the technical training specific to their position, must ensure that they are aware of the practices, policies, procedures and requirements in terms of information security and operations of their site, knowing the consequences of a deviation from established procedures. Training and information documents will be provided at the time of initial incorporation and each time they are modified.

The trusted roles System Administrators who perform tasks related to cryptographic devices (HSMs) require special training in the operation of HSMs.

3.3.4. Requirements and frequency of the training update

The TSA draws up an annual Training Plan where the training needs of the staff are detected and planned in the appropriate way.

3.3.5. Penalties for unauthorized actions

The disciplinary process is specified in the TSA's internal procedure based on Royal Legislative Decree 2/2015, of 23 October, approving the revised text of the Workers' Statute Act, which will be applied to purge responsibilities arising from unauthorized actions.

3.3.6. Independent recruitment requirements

The hiring of personnel through a third-party company will comply with the requirements established in this DP and in the internal procedures of the technology provider. The Consorci AOC is responsible, in any case, for the effective execution.

These aspects are specified in the legal instrument used to agree on the provision of services by a third party other than the technology provider.

3.3.7. Documentation provided to staff

The TSA will provide staff with general documentation of the services and specific to the job to be carried out (operating manuals, technical or programming procedures, support procedures, etc.) so that they can competently carry out their functions.

4. Applicable

The Consorci AOC establishes in its legal instruments with its subscribers and verifiers that the law applicable to the provision of the service is as follows:

- Law 29/2010, of 3 August, on the use of electronic media in the public sector of Catalonia.
- Law 26/2010, of 3 August, on the legal regime and procedure of the public administrations of Catalonia.
- 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.
- Regulation (EU) 2024/1183 of the European Parliament and of the Council of April 11, 2024 amending Regulation (EU) No. 910/2014 with regard to the establishment of the European digital identity framework
- Commission Implementing Regulation (EU) 2025/1929 of 29 September 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the binding of date and time to data and establishing the accuracy of the time sources for the provision of qualified electronic time stamps
- Law 6/2020, of 11 November, regulating certain aspects of electronic trust services.
- Law 39/2015, of 1 October, on the Common Administrative Procedure of Public Administrations.
- Law 40/2015, of 1 October, on the Legal Regime of the Public Sector.
- Royal Decree 203/2021, of 30 March, approving the Regulation on the action and operation of the public sector by electronic means.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).
- Organic Law 3/2018, of 5 December, on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD).
- Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010 and repealing Directive 2007/64/EC.
- Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 laying down minimum technical specifications and procedures for the security levels of electronic identification means in accordance with Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.
- Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down rules for the assessment of the security of qualified signature and seal creation devices in accordance with Article 30(3) and Article 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council, on electronic identification and trust services for electronic transactions in the internal market.

- Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open communication standards.
- Royal Decree 311/2022, of 3 May, regulating the National Security Scheme.
- The Information Security Regulatory Framework of the Cybersecurity Agency of Catalonia within the scope of the Generalitat de Catalunya, which determines the strategic lines, policies, standards and security guides of the Generalitat de Catalunya, on a supplementary basis in the absence of its own.
- Consorci AOC Security Policy.

5. Other requirements

As not specified in this document, time stamping services under this DP are governed by what is specified in the documents "Consorci AOC Certification Authority Certification Practice Statement (CPP), "Consorci AOC Certification Policy for Devices and Infrastructures" and "Description of Consorci AOC Certificate Profiles" published on the https://epscd.aoc.cat/ca/index.html#politiques https://epscd.aoc.cat/ca/index.htmlwebsite, in so far as it is not applicable exclusively to the certificate issuance services of the Consorci AOC, and in so far as it is applicable to the certificates of the Consorci AOC's time stamping services (see OID certificate policies in point 1.2).