Administració Oberta de Catalunya

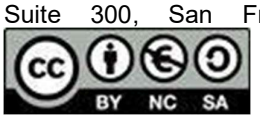
Declaració de pràctiques del Servei de segellat de temps

Generalitat de Catalunya

Localret

Administració Oberta de Catalunya

Control documental

Estat formal	Aprovat
Elaborat per	Consorci AOC
Aprovat per	Comissió Executiva del Consorci AOC el 18 de Desembre de 2024
Data de creació	18/12/2024
Nivell d' accés a la informació	Pública
Títol	Declaració de pràctiques del Servei de segellat de temps
Fitxer	DP_TSA-2.0-CAT.docx
Control de còpies	Només les còpies disponibles a la Seu electrònica del Consorci AOC garanteixen l' actualització dels documents. Tota còpia impresa o guardada en ubicacions diferents es consideraran còpies no controlades.
Drets d'autor	

Control de versions

Versió	Descripció	Data
1.0	Versió inicial	18/12/2024
2.0	Incorporació servei no qualificat	17/12/2025

Administració Oberta de Catalunya

Index

Administració Oberta de Catalunya

1. Introducció

1.1. Vista general

El present document constitueix la Declaració de Pràctiques (en endavant, DP) dels següents serveis d'expedició de segells electrònics de temps (en endavant, serveis de segellat de temps) prestats pel Consorci Administració Oberta de Catalunya (en endavant, Consorci AOC):

- **SERVEI D'EXPEDICIÓ DE SEGELLS ELECTRÒNICS QUALIFICATS DE TEMPS** (en endavant, servei de segellat qualificat de temps)
- **SERVEI D'EXPEDICIÓ DE SEGELLS ELECTRÒNICS NO QUALIFICATS DE TEMPS** (en endavant, servei de segellat no qualificat de temps)

La prestació d'aquests serveis es realitza d'acord amb el Reglament (UE) nº 910/2014 del Parlament Europeu i del Consell, de 23 de juliol de 2014, relatiu a la identificació electrònica i els serveis de confiança per a les transaccions electròniques en el mercat interior i pel qual es deroga la Directiva 1999/93/CE, modificat pel Reglament (UE) 2024/1183, d'11 d'abril de 2024 (en endavant, Reglament eIDAS) i amb la Llei 6/2020, d'11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança (en endavant, Llei 6/2020).

En el que no està especificat en aquest document, els serveis de segellat de temps sota aquesta DP es regeixen per l'especificat en els documents "Declaració de Pràctiques de Certificació (DPC) Autoritat de Certificació del Consorci AOC", "Política de Certificació per a Dispositius i Infraestructures Consorci AOC" i "Descripció dels perfils de Certificats Consorci AOC" publicats a la pàgina web https://epscd.aoc.cat/ca/index.html#politiques, en el que no sigui aplicable exclusivament als serveis d'expedició de certificats del Consorci AOC, i en el que sigui aplicable als certificats dels serveis de segellat de temps del Consorci AOC (veure OID polítiques de certificats en punt 1.2).

Per prestar els serveis d'expedició de segells electrònics de temps, el Consorci AOC subcontracta un proveïdor extern (en endavant, el proveïdor tecnològic) el hosting, la gestió i l'operació dels serveis de segellat de temps sota aquesta DP.

Els serveis de segellat de temps sota aquesta DP permeten obtenir una marca de temps fiable i segura amb totes les garanties, tant jurídiques com tècniques, que estableix la normativa vigent. Aquests serveis permeten acreditar, mitjançant la marca de temps que reporta el servei, l'existència d'un element en format electrònic (document, signatura, etc.) en un instant determinat del temps. Entre els avantatges que suposen aquests serveis destaquen:

- Seguretat: el segell de temps és una manera segura i fiable d'obtenir marques temporals i alhora vincular-les a un document. La data i l'hora del segell de temps està protegida per mecanismes robustos de seguretat (signatura digital).
- Tercer de confiança: cada segell de temps que s' emet està garantit per un tercer de confiança, en aquest cas el Consorci AOC i CATCert.
- Evidència electrònica: cada segell de temps és una evidència electrònica que acredita un instant temporal en el qual es pot assegurar l' existència d' un document.
- Estalvi: el Consorci AOC assumeix el cost del servei i l'ofereix lliure de cost per a les aplicacions del sector públic català.

Els segells de temps emesos sota aquesta DP són conformes a la Política BTSP (Best practices Time-Stamp Policy) definida en l'estàndard europeu ETSI EN 319 421, identificada mitjançant l'OID 0.4.0.2023.1.1.

Els segells de temps emesos sota aquesta DP inclouen l' OID de la Política BTSP 0.4.0.2023.1.1.

La precisió dels segells de temps emesos sota aquesta DP serà d'1 segon respecte a l'hora UTC.

Les peticions, les respostes i els certificats dels serveis de segellat de temps sota aquesta DP són conformes a l' estàndard europeu ETSI EN 319 422.

1.2. Nom del document i identificació

Aquest document té les següents dades d'identificació:

Nom	Declaració de Pràctiques del Servei de Segellat de Temps del Consorci AOC
Versió	2.0
OID Declaració de Pràctiques del Servei de Segellat de Temps	1.3.6.1.4.1.15096.3.2
OID Política del Servei de Segellat Qualificat de Temps	0.4.0.2023.1.1 (ETSI EN 319 421 BTSP)
OID Política del Servei de Segellat no Qualificat de Temps	0.4.0.2023.1.1 (ETSI EN 319 421 BTSP)
OID Polítiques de Certificats del Servei de Segellat Qualificat de Temps (Certificats de TSU)	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 Polítiques de Certificats del Servei de Segellat no Qualificat de Temps (Certificats de TSU)	1.3.6.1.4.1.15096.1.3.2.113 (Consorci AOC)
Localització	https://tsa.aoc.cat/regulacio/

1.3. Participants

1.3.1. Autoritat de Segellat de Temps (TSA)

Una Autoritat de Segellat de Temps (TSA, Time-Stamping Authority) és un Prestador de Serveis de Confiança que presta serveis de segellat de temps. El paper d'una TSA és convertir-se en un tercer de confiança certificant l'existència de les dades segellades en una data i hora concretes.

Una TSA opera una o diverses Unitats de Segellat de Temps (TSU, Time-Stamping Units) per a cadascun dels serveis de segellat de temps que presta.

La TSA serà el responsable de la prestació dels serveis de segellat de temps sota aquesta DP, i del compliment de les seves obligacions i de les obligacions de totes les organitzacions externes utilitzades per prestar part d' aquests serveis.

El Consorci AOC actua com a TSA sota aquesta DP.

1.3.2. Subscriptor

És una entitat del Sector Públic de Catalunya que demana l'ús d'un servei de segellat de temps sota aquesta DP, a qui se li expedeixen segells de temps.

Comprendrà tant a les aplicacions del propi Subscriptor com a les persones físiques (usuaris finals) que en depenguin i que podran realitzar sol·licituds de segells de temps a la TSA utilitzant els seus propis recursos i mitjans, les quals assumeixen el compliment d'algunes obligacions del Subscriptor, sense perjudici de la responsabilitat del Subscriptor, en cas d'incompliment d'aquestes obligacions.

1.3.3. Tercer que confia

És la persona física o entitat (amb o sense personalitat jurídica) que rep una transacció electrònica amb un segell de temps emès per un servei de segellat de temps sota aquesta DP, i que voluntàriament confia en aquest segell de temps (Relying party).

1.4. Obligacions dels participants

1.4.1. Obligacions de la TSA

El Consorci AOC, actuant com a TSA sota aquesta DP, té les obligacions següents en els serveis de segellat de temps que presta:

- Prestar els serveis i emetre els segells de temps d'acord amb aquesta DP.
- Mantenir publicada la documentació especificada al punt 1.5.5.
- Modificar aquest document i notificar, si s'escau, les modificacions conforme a l'especificat al punt 1.5.6.
- Mantenir publicats els certificats associats a les claus privades utilitzades per a la signatura dels segells de temps (certificats de TSU).
- Totes les que es derivin del contingut dels documents "Declaració de Pràctiques de Certificació (DPC) Autoritat de Certificació del Consorci AOC" i "Política de Certificació per a Dispositius i Infraestructures Consorci AOC" que sigui aplicable (vegeu punt 1.1), així com de la legislació vigent.

1.4.2. Obligacions de les organitzacions externes que presten part dels serveis

El Consorci AOC, per al hosting, la gestió i l' operació i el monitoratge dels serveis de segellat de temps que presta sota aquesta DP, utilitza els serveis d' organitzacions externes que estan subjectes a les obligacions següents:

- Gestió i operació (el proveïdor tecnològic)

- Complir amb els acords dels contractes subscrits amb el Consorci AOC.
- Controlar i supervisar el funcionament dels serveis per garantir que es presten d'acord amb aquesta DP.
- Instal·lar, configurar, mantenir, operar i consultar registres d'auditoria dels elements maquinari i programari dels serveis.
- Establir les mesures i controls de seguretat necessaris per protegir el sistema i les claus privades dels serveis.
- Executar els serveis emprant els mitjans tècnics i materials adequats, així com el personal qualificat requerit pels estàndards aplicables.
- Complir els nivells de qualitat dels serveis requerits pels estàndards aplicables, quant a aspectes tècnics, operacions i de seguretat es refereix.
- Garantir que els segells de temps emesos són fidels a la informació en les corresponents peticions.
- Garantir la data i hora dels segells de temps emesos amb una precisió d'1 segon respecte a l'hora UTC.
- Emmagatzemar i custodiar els registres d'auditoria dels elements maquinari i programari dels serveis, en el cas de les peticions i respostes, durant el període mínim establert en el punt 2.10.
- Complir amb els acords de nivell de servei (SLA, Service Level Agreements) de disponibilitat, monitoratge d'infraestructures i suport a incidències 24x7.
- Totes les que es derivin de la legislació vigent.

- Centres de Procés de Dades (CPD)
  - Complir amb els acords dels contractes subscrits amb el proveïdor tecnològic.
  - Prohibir l'accés a l' àrea dels serveis a qualsevol tercer aliè al personal del centre de dades o autoritzat pel proveïdor tecnològic i mantenir en tot moment un registre de les persones autoritzades pel proveïdor tecnològic que accedeixen a l'Àrea de Servei.
  - Complir les indicacions donades pel proveïdor tecnològic i acordades amb el CPD respecte al maneig dels seus equips.
  - No tenir cap tipus de control sobre la informació dels serveis transmesa a través de les instal·lacions, ni examinar l'ús que els clients dels serveis fan de les dades, ni conèixer el tipus d'informació que envien, reben o emmagatzemen.
  - Complir amb els SLA de disponibilitat, monitoratge d'infraestructures i suport a incidències 24x7.
  - Totes les que es derivin de la legislació vigent.
- Computació al núvol
  - Complir amb els acords dels contractes subscrits amb el proveïdor tecnològic.
  - Ubicació de servidors a la Unió Europea.
  - Doble factor d'autenticació per als administradors del servei amb política de contrasenyes.
  - Control d' accés definit per a cada aplicació i tipus d'usuari.

- Complir amb els SLA de disponibilitat, monitoratge d'infraestructures i suport a incidències 24x7.
- Totes les que es derivin de la legislació vigent.

1.4.3. Obligacions del Subscriptor

Les obligacions del Subscriptor d' un servei de segellat de temps sota aquesta DP són:

- Complir amb el que estableixen les Condicions Generals de Prestació de Serveis del Consorci AOC i les Clàusules de Divulgació del servei de segellat de temps.
- Utilitzar el servei d' acord amb aquesta DP.
- Custodiar de forma diligent les claus secretes, contrasenyes o pins utilitzats per a la identificació i autenticació del Subscriptor al servei, prenent les precaucions raonables per evitar la seva pèrdua, revelació, modificació o ús no autoritzats.
- Adequar els seus sistemes d'informació als requeriments fixats en la documentació tècnica d' integració per realitzar les sol.licituds al servei, conforme a l' especificat en el punt 2.5, i per tractar les seves respostes, conforme a l' especificat en el punt 2.6.
- Validar els segells de temps continguts en les respostes del servei conforme a l'especificat en el punt 2.7, en el moment de recepció de les respostes.
- Informar immediatament la TSA sobre qualsevol de qualsevol incident o fet que afecti el servei prestat o que pugui afectar la validesa dels segells de temps.
- Tenir en compte les limitacions d'ús especificades en el punt 1.7.
- Informar degudament els usuaris finals de les obligacions anteriors.
- Designar un responsable de l'ens, i un responsable tècnic per a cadascuna de les aplicacions sota l'adscripció de l'ens que actuïn com a consumidores del servei.

1.4.4. Obligacions del Tercer que confia

Les obligacions del Tercer que confia en un segell de temps emès per un servei de segellat de temps sota aquesta DP són:

- Validar el segell de temps conforme a l'especificat en el punt 2.7, en el moment actual o, si s'escau, en el moment en què s'ha protegit la integritat del segell de temps (per exemple, mitjançant un segell de temps addicional, o emmagatzemant el segell de temps de forma segura).
- Tenir en compte les limitacions d'ús especificades en el punt 1.7.

1.5. Administració del document

1.5.1. Organització

La redacció, publicació, revisió i modificació d'aquesta DP és responsabilitat de:

Organització	Consorci Administració Oberta de Catalunya (Consorci AOC)
E-mail	suport@aoc.cat
Pàgina Web	https://www.aoc.cat

1.5.2. Dades de contacte

Per a qualsevol consulta sobre aquesta DP, es pot contactar amb:

Organització	Consorci Administració Oberta de Catalunya (Consorci AOC)
Responsable	Responsable dels Serveis de Segellat de Temps del Consorci AOC
E-mail	scd@aoc.cat
Telèfon	+34 93 272 40 00 - 900 90 50 90

1.5.3. Responsable per determinar la idoneïtat de la DP amb les Polítiques

El Responsable del Servei de Certificació Digital del Consorci AOC és el responsable de determinar la idoneïtat de la DP amb les Polítiques.

1.5.4. Procediment d' aprovació

El sistema documental i d' organització del Consorci AOC garanteix, mitjançant l'existència i l'aplicació dels corresponents procediments, el correcte manteniment de la DP i de les especificacions del procediment de publicació d' especificacions de servei.

La versió inicial d'aquesta DP és aprovada per la Comissió Executiva del Consorci AOC, que és l'òrgan col·legiat de direcció executiva del Consorci AOC. El director gerent del Consorci AOC és competent per aprovar-ne les successives modificacions.

1.5.5. Documentació publicada

El Consorci AOC posa a disposició de totes les parts interessades, en el repositori públic https://tsa.aoc.cat/regulacio/, la següent documentació dels serveis de segellat de temps sota aquesta DP:

- Aquesta DP.
- Les Clàusules de Divulgació.

El Consorci AOC publica, un cop aprovada i vigent, qualsevol nova versió d'aquesta documentació, mantenint publicades totes les seves versions anteriors.

1.5.6. Modificacions

Aquest document es modificarà quan es produeixin canvis rellevants en la prestació dels serveis subjectes a ell o quan es realitzin revisions del document. Es produirà almenys una revisió biennal del document, en cas que no es produeixin abans canvis rellevants en la prestació dels serveis. Els canvis i les revisions quedaran reflectits en el quadre de control de versions a l'inici del document.

Les modificacions d'aquest document es notificaran als Subscriptors i als Tercers que confien, quan els canvis en la prestació dels serveis incideixin directament en els seus drets i obligacions, d' acord amb el que estipula les Clàusules de Divulgació dels serveis. La notificació de les modificacions podrà ser publicada pel Consorci AOC al repositori públic https://tsa.aoc.cat/regulacio/.

1.6. Responsabilitat

El Consorci AOC serà responsable dels perjudicis causats de forma deliberada o per negligència a qualsevol persona física o entitat (amb o sense personalitat jurídica) a causa de l'incompliment de les obligacions establertes en el Reglament eIDAS i la Llei 6/2020 respecte als serveis de segellat de temps sota aquesta DP.

Aquesta responsabilitat queda limitada per:

- Causes de fora major.
- Ús indegut del servei.
- Per l'incompliment de les obligacions del Subscriptor o del Tercer que confia establertes en aquesta DP, així com en les Condicions Generals de Prestació de Serveis del Consorci AOC i les Clàusules de Divulgació del servei.

1.7. Limitacions d' ús

- Els segells de temps emesos pels serveis de segellat de temps sota aquesta DP estan dirigits a ser usats en l'àmbit de totes les Administracions Públiques Catalanes, per garantir l'existència de les signatures electròniques i els segells electrònics que es presenten davant les Administracions Públiques Catalanes en un moment determinat del temps, així com per garantir les transaccions i la imputabilitat en processos entre ciutadans, empreses i les mateixes administracions.
- Els serveis de segellat de temps sota aquesta DP no emmagatzemen ni custodien els segells de temps emesos, però emmagatzemen i custodien registres d' auditoria de les peticions i respostes dels serveis que permeten identificar els segells de temps emesos.
- El Consorci AOC no ofereix cap programari, llibreria o servei per realitzar les sol·licituds als serveis de segellat de temps sota aquesta DP, conforme a l'especificat en el punt 2.5, ni per tractar les seves respostes, conforme a l'especificat en el punt 2.6, sent responsabilitat del Subscriptor o dels seus usuaris finals adaptar els seus sistemes o utilitzar programari existent en el mercat per realitzar les sol·licituds i tractar les respostes.

2. Requisits operacionals

2.1. Funcionament del servei de segellat de temps

El servei de segellat de temps fa servir el protocol definit a l'estàndard RFC 3161 sobre una comunicació HTTPS, conforme a l'estàndard europeu ETSI EN 319 422.

Els passos del protocol són:

- El client envia una petició de segell de temps contenint el hash de les dades a segellar a una URL específica del servei, segons el format establert en l'estàndard RFC 3161.
- El servei verifica la petició i, si és vàlida, emet el segell de temps, per a la qual cosa signa el hash de les dades a segellar juntament amb la data i hora actual i altres dades amb la clau privada associada a un certificat de segell de temps actiu del servei, segons el format establert a l'estàndard RFC 3161.
- El segell de temps es remet al client de forma síncrona en una resposta a la petició, segons el format establert en l'estàndard RFC 3161.

El client té l'obligació de validar el segell de temps emès pel servei, d'acord amb el que especifica el punt 2.7.

2.2. Claus privades i certificats de segellat de temps

Les claus privades utilitzades per a la signatura dels segells de temps (claus privades de segellat de temps o claus privades de TSU) es generen i custodien en un dispositiu criptogràfic segur (HSM) amb la certificació Common Criteria EAL 4 o superior, o FIPS 140-3 Level 3.

Els certificats associats a les claus privades utilitzades per a la signatura dels segells de temps (certificats de segellat de temps o certificats de TSU) són certificats de segell electrònic emesos pel Consorci AOC sota les polítiques de certificats del servei de segellat de temps (veure OID en punt 1.2), conforme a l'estàndard ETSI EN 319 422, i d'acord amb els documents "Declaració de Pràctiques de Certificació (DPC) Autoritat de Certificació del Consorci AOC", "Política de Certificació per a Dispositius i Infraestructures Consorci AOC" i "Descripció dels perfils de Certificats Consorci AOC" publicats a la pàgina web https://epscd.aoc.cat/ca/index.html#politiques.

Pel servei de segellat de temps qualificat els certificats seran qualificats amb acord al que estableix la norma ETSI EN 319 411-2.

Els certificats qualificats de segellat de temps tindran un període de validesa de 5 anys i els no qualificats de 10. Les claus privades de segellat de temps qualificat tindran un període de validesa de 2 anys i de 5 anys pel cas del servei no qualificat. Abans de la fi del període de validesa d'una clau privada, es generaran noves claus i s'emetrà un nou certificat que substituiran els anteriors en la signatura dels segells de temps, garantint així una validesa mínima dels segells de temps de 3 anys en el servei de segell de temps qualificat i de 5 anys en el servei no qualificat, si no es produeix una revocació del certificat abans de la seva expiració.

Un cop finalitzat el període de validesa d' una clau privada de segellat de temps i abans de l'expiració del certificat associat, la clau privada serà destruïda, incloent-hi totes les seves còpies, de la manera següent que impedeix la seva recuperació:

- Es realitzarà un esborrat segur de la clau privada en els dispositius criptogràfics (HSM) que la tinguin emmagatzemada, seguint els passos descrits en el manual d'administració dels HSM.

- Es realitzarà una esborrat assegurança de totes les còpies de seguretat de la clau privada.

Una clau privada i un certificat de segellat de temps poden estar en un dels tres estats següents:

- Actiu: mentre la clau privada s' està fent servir per signar segells de temps.
- Desactivat: quan la clau privada s' ha deixat d' usar per signar segells de temps, abans de la fi del seu període de validesa.
- Acabat: quan la clau privada s' ha destruït i el certificat ha expirat o ha estat revocat.

Els certificats de segellat de temps del Consorci AOC, tant els actuals, en estat actiu, com els anteriors, en estat desactivat o acabat, es troben publicats a la pàgina web https://tsa.aoc.cat/regulacio/.

El servei qualificat de segell de temps emprarà els següents certificats electrònics de TSU, per prestar el servei, amb OID de política 1.3.6.1.4.1.15096.1.3.2.112:

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

  Emissor: "SubCA Q TSA (G3) A.5"

  Algoritme i longitud de la clau: RSA 2048

  Validesa: 5 anys. Fins el 3 de novembre de 2029.

  Període d'ús de la clau privada: 2 anys. Fins el 3 de novembre de 2026

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

  Algoritme i longitud de la clau: RSA 3072
  Validesa: 5 anys. Fins el 15 de desembre de 2030.
  Període d'ús de la clau privada: 2 anys. Fins el 15 de desembre de 2027

Pel que fa al servei no qualificat de segell de temps, amb **OID de política 1.3.6.1.4.1.15096.1.3.2.113,** el certificat de TSU serà el següent**:**

Subject: CN=CONSORCI AOC TSU 2025, organizationIdentifier=VATES-Q0801175A, O=CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA, C=ES
Emissor: "SubCA TSAnoQ (G3) A.6"
Algoritme i longitud de la clau: RSA 3072
Validesa: 10 anys. Fins el 15 de desembre de 2035
Període d'ús de la clau privada: 5 anys. Fins el 15 de desembre de 2030

2.3. Unitat de segellat de temps (TSU)

Una Unitat de Segellat de Temps (TSU, Time-Stamping Unit) és un conjunt de maquinari i programari que és gestionat com una unitat i té una única clau de signatura de segells de temps activa en un instant de temps (clau privada de segellat de temps o clau privada de la TSU).

Els segells de temps són emesos per les TSU dels serveis de segellat de temps prestats per la TSA.

Un servei de segellat de temps només tindrà una TSU activa, excepte durant el període transitori de substitució de les claus i el certificat del servei (substitució de TSU), durant el qual podran

estar actives l'anterior TSU, amb les anteriors claus i l'anterior certificat, i la nova TSU, amb les noves claus i el nou certificat.

2.4. Control d' accés

El control d' accés al servei de segellat de temps per part dels Subscriptors es realitza per nom d' usuari i contrasenya.

2.5. Sol·licitud de segell de temps

Per realitzar una sol·licitud de segell de temps, el client haurà d'enviar una petició contenint el hash de les dades a segellar a una URL específica del servei de segellat de temps proporcionada pel Consorci AOC.

L' enviament de la petició es realitzarà sobre una comunicació HTTPS autenticada amb nom d' usuari i contrasenya.

La petició haurà d' utilitzar la sintaxi definida en l' estàndard RFC 3161, conforme a l' estàndard europeu ETSI EN 319 422.

2.6. Format de la resposta

La resposta del servei de segellat de temps utilitza la sintaxi definida en l' estàndard RFC 3161, conforme a l' estàndard europeu ETSI EN 319 422.

Si no hi ha cap error, la resposta inclou el segell de temps emès, signada amb la clau privada de la corresponent TSU activa, que conté, entre altres dades, el mateix valor del hash de les dades a segellar en la petició i la data i hora actual del servidor de la TSU que processa la petició.

El segell de temps emès conté l' OID de la Política BTSP 0.4.0.2023.1.1.

En el cas del servei de segellat qualificat del temps, el segell de temps emès conté l' extensió qcStatements amb el valor especificat en l' estàndard europeu ETSI EN 319 422 per als segells qualificats de temps.

Davant de qualsevol error, la resposta inclourà el corresponent codi d' error definit en l' estàndard RFC 3161.

2.7. Validació del segell de temps

La validació d' un segell de temps haurà de ser realitzada per la part interessada pels seus propis mitjans, utilitzant les dades segellades i el certificat de la TSU amb la clau privada de la qual s' ha signat el segell de temps.

Els certificats de les TSU del Consorci AOC, tant els actuals, en estat actiu, com els anteriors, en estat desactivat o acabat, es troben publicats a la pàgina web https://tsa.aoc.cat/regulacio/.

Per validar un segell de temps en un moment determinat, s' hauran de realitzar les següents verificacions:

- El hash de les dades contingudes en el segell de temps és igual al hash de les dades segellades.
- La signatura digital del segell de temps és correcta.
- La clau privada de la TSU usada per signar el segell de temps no ha estat compromesa abans del moment de la validació del segell de temps. Per realitzar aquesta verificació:

Durant el període de validesa del certificat de la TSU (abans de la seva expiració), es pot consultar el seu estat de revocació a través del servei d'OCSP o CRL, conforme als procediments indicats en el document "Declaració de Pràctiques de Certificació (DPC) Autoritat de Certificació del Consorci AOC" publicat a la pàgina web https://epscd.aoc.cat/ca/index.html#politiques.

- Després del període de validesa del certificat de la TSU (després de la seva expiració), es pot consultar el seu estat de revocació únicament a través del servei d'OCSP, ja que aquest retorna l'estat revocat dels certificats després de la seva expiració (la CRL no manté els certificats revocats després de la seva expiració), i la TSA pot garantir que la clau privada de la TSU no ha estat compromesa després de l'expiració del certificat de la TSU.
- El Consorci AOC garanteix que les claus privades dels seus TSU no han estat compromeses després de l' expiració dels respectius certificats de TSU mitjançant la destrucció de les claus privades abans de l' expiració dels certificats.

- Els algoritmes de hash utilitzats en el segell de temps (en el hash de les dades segellades i en la signatura del segell de temps), i l'algoritme i la mida de clau de la firma del segell de temps es poden continuar considerant segurs en el moment de la validació del segell de temps.
- En el cas del servei de segellat qualificat de temps, el certificat de la TSU ha estat emès per una Autoritat de Certficació (CA, Certification Authority) del Consorci AOC el certificat del qual està inclòs en la llista de confiança (TSL, Trust-service Status List) espanyola, en un servei de segellat qualificat de temps en estat granted en el moment de la validació del segell de temps o en el moment de l'emissió del segell de temps, conforme al Reglament eIDAS i a l' estàndard europeu ETSI TS 119 612.

Les Administracions Públiques Catalanes podran dur a terme aquestes verificacions utilitzant el Servei Validador que ofereix el mateix Consorci AOC.

En cas de produir-se un incident de seguretat per compromís o sospita de compromís de la clau privada de la TSU usada per signar el segell de temps o per pèrdua de calibratge del rellotge del servidor que ha emès el segell de temps, es pot considerar que el segell de temps és vàlid, si la TSA confirma que el segell de temps no ha estat afectat per l' incident.

2.8. Sincronització de temps

Es realitza una sincronització del rellotge dels servidors de les TSU amb dues fonts de temps UTC Stratum 1 mitjançant el protocol NTP (RFC 5905 Network Time Protocol Version 4), monitoritzant en tot moment aquesta sincronització:

- Secció d'Hora del Reial Institut i Observatori de l'Armada a San Fernando (ROA)
- Servei de sincronització horària del Centre Informàtic Científic d'Andalusia (CICA)

La precisió declarada de l' hora en els segells de temps amb l' hora UTC és d' 1 segon. Els servidors de les TSU no emetran segells de temps en cas de detectar una possible diferència més gran entre els seus rellotges i les fonts de temps UTC amb les quals se sincronitzen.

2.9. Algorismes de hash

L' algoritme de hash utilitzat pel client en la petició per representar les dades que s' han de segellar podrà ser RIPEMD-160, SHA-1, SHA-256, SHA-384 o SHA-512. D' acord amb la norma

ETSI TS 119 312 i la Guia CCN-STIC 807, es recomana utilitzar l' algoritme de hash SHA-256, SHA-384 o SHA-512.

L' algoritme de hash utilitzat en la signatura del segell de temps contingut en la resposta del servei és SHA-256.

2.10. Registres d' auditoria

La TSA recull registres d' auditoria dels sistemes que intervenen en els serveis de segellat de temps, genèrics i específics dels serveis.

Els registres d' auditoria genèrics inclouen, entre d' altres, els esdeveniments relatius a:

- Accés a les zones de seguretat
- Accés als sistemes de la infraestructura
- Operacions criptogràfiques

Els registres d' auditoria específics dels serveis de segellat de temps inclouen tots els esdeveniments relatius a:

- Peticions i respostes.
- Cicle de vida de les claus i els certificats de les TSU.
- Sincronització i detecció de pèrdua de sincronització del rellotge dels servidors de les TSU amb les fonts de temps UTC.

El Consorci AOC mantindrà els registres d' auditoria de les peticions i respostes durant un període mínim 5 anys per al servei no qualificat de temps i de 15 anys, per al servei de segellat qualificat de temps, des de l' expiració del certificat del servei actiu en el moment de l' operació o des de la finalització del servei.

2.11. Incidents de seguretat

El Pla de Recuperació davant Desastres del Consorci AOC contempla els casos d' incidents de seguretat per compromís o sospita de compromís de la clau privada d' una TSU i per pèrdua de calibratge del rellotge d' un servidor d' una TSU, que puguin haver afectat segells de temps emesos.

En cas de produir-se algun d' aquests incidents de seguretat, el Consorci AOC proporcionarà als Subscriptors i Tercers que confien informació que pot ser utilitzada per identificar els segells de temps que puguin haver estat afectats.

2.12. Cessament d' activitat

El Consorci AOC compta amb un Pla de Cessament on s' estableixen les accions a realitzar per al cessament de l' activitat dels serveis de segellat de temps, incloent-hi la revocació de tots els certificats vigents i la destrucció de totes les claus privades de les TSU dels serveis, tant els actuals, en estat actiu, com els anteriors, en estat desactivat (els certificats anteriors en estat acabat no són vigents, i les claus privades anteriors en estat acabat ja han estat destruïdes).

El cessament dels serveis es comunicarà prèviament als Subscriptors i totes les parts interessades amb les quals el Consorci AOC tingui acords o altre tipus de relacions, en el cas del servei de segellat qualificat de temps, amb l' antelació mínima legalment requerida.

3. Controls de seguretat física, de procediments i de personal

3.1. Controls de seguretat física

Les instal·lacions que alberguen la infraestructura dels serveis de segellat de temps gestionada pel proveïdor tecnològic estan subjectes a les validacions anuals de la norma UNE-ISO/IEC 27001, la qual regula l'establiment de processos adequats per garantir una correcta gestió de la seguretat en els sistemes d'informació.

3.1.1. Situació i característiques del CPD

La infraestructura dels serveis de segellat de temps gestionada pel proveïdor tecnològic es troba ubicada en dos centres de dades (CPD) que garanteixen la disponibilitat 24x7 dels sistemes de comunicació i la disponibilitat dels sistemes dels serveis.

Els CPD estan ubicats dins del territori de la Unió Europea.

3.1.2. Control d' accés físic

Els CPD compten amb les següents mesures de seguretat física:

- Videovigilància i videogravació perimetral en accessos, pàrquing i àrees d'instal·lacions.
- Personal 24x7 al centre.
- Control d' accés a l' edifici:
    - El CPD compta amb un sistema de control d' accés que garanteix l' accés segur 24x7x365 al personal autoritzat del proveïdor tecnològic a l ' àrea de servei contractada.
    - Els accessos es registren individualment amb dades personals del personal autoritzat del proveïdor tecnològic.
    - L'accés multinivell està restringit a totes les àrees sensibles del centre, amb targeta sense contacte, empremta dactilar i/o clau.
    - L' accés a les zones de seguretat està protegit amb control dual i monitoritzat constantment mitjançant CCTV i sensors d' obertura de la zona.

3.1.3. Alimentació elèctrica i climatització

Els CPD compten amb serveis d' energia d' alta disponibilitat amb les infraestructures següents:

- Sales d' UPS alterna amb UPS de 120kvAs en configuració 2N.
- Grups electrògens de suport en configuració N + 1.
- Dipòsits de fuel per a una autonomia de més de 48 hores de funcionament en el CPD.
- Quadres elèctrics de sala alimentats des dels grups d' UPS independents.

Les Sales Tècniques estan climatitzades amb equips partits de condensació per aire, amb impulsió d' aire per fals sòl i humidificador de l' ambient, amb expansió directa redundant i

independent a cada sala, en configuració N + 1 rotatiu. L' aportació d' aire exterior per a ventilació de les sales del CPD es pren de la xarxa de conductes provinent del ventilador d' impulsió d' aire exterior, que passa a través d' una unitat de filtratge que manté les condicions biològiques i de substàncies químiques actives.

3.1.4. Exposició a l' aigua

Els CPD s'ubiquen en una zona on el risc d'inundació és nul, estant situat a 1500 metres d'una àrea de risc de tipus 5, freqüència baixa (menys de 500 anys).

3.1.5. Protecció i prevenció d' incendis

El sistema d'extinció d'incendis dels CPD cobreix sales tècniques i instal·lacions crítiques:

- Sistemes de detecció constituïts per detectors iònics de fums i gasos de combustió.
- Zones de detecció controlades per central analògica microprocessada modular amb plena autonomia de senyalització, centralització de foc i avaria.
- Agent extintor FE-13

3.1.6. Media storage

Cada mitjà d'emmagatzematge desmuntable (cintes, cartutxos, CD, discos, etc.) roman només a l'abast de personal autoritzat per les mesures d'accés físic al CPD i a l'armari RACK corresponent.

3.1.7. Eliminació dels suports d' informació

Quan hagi deixat de ser útil, la informació sensible és destruïda de la forma més adequada al suport que la contingui:

- Impresos i paper: mitjançant trituradores o en papereres disposades a l' efecte per a la seva posterior destrucció controlada.
- Mitjans d' emmagatzematge: abans de ser rebutjats o reutilitzats, han de ser processats per assegurar que la informació continguda ha estat eliminada de forma segura.

3.1.8. Off-site backup

Es mantindrà una còpia de seguretat en un CPD diferent des del qual es realitza la prestació del servei amb una freqüència menor a 7 dies.

3.2. Controls de procediments

3.2.1. Rols de confiança

En la següent taula s' indiquen els rols de confiança dels serveis de segellat de temps sota aquesta DP, conforme a l' especificat en l' estàndard ETSI EN 319 401:

ROL DE CONFIANÇA	DESCRIPCIÓ
Responsables de Seguretat (*Security Officers*)	Responsables generals d' administrar l' aplicació de les pràctiques de seguretat.
Administradors de Sistemes (*System Administrators*)	Autoritzats per instal·lar, configurar i mantenir els sistemes de confiança del PSC per a la gestió dels serveis. Això inclou la recuperació del sistema.
Operadors de Sistemes (*System Operators*)	Responsables d' operar els sistemes de confiança del TSP en el dia a dia. Autoritzats per realitzar còpies de seguretat del sistema.
Auditors de Sistemes (*System Auditors*)	Autoritzats per veure els arxius i els registres d'auditoria (*logs*) dels sistemes de confiança del TSP.

3.2.2. Nombre de persones requerides per tasca

Es requereixen almenys dues persones per a l'execució de les tasques de cada rol de confiança classificades com a crítiques per als serveis de segellat de temps sota aquesta DP, com les tasques relatives als dispositius criptogràfics (HSM) on es generen i es fan servir les claus privades dels serveis.

3.2.3. Identificació i autentació per a cada rol

Cada rol té assignada una o diverses persones, si s' escau, designades per la direcció del Consorci AOC o del proveïdor tecnològic.

Cada persona només controla els actius necessaris per al seu rol, assegurant així que cap persona accedeix a recursos no assignats.

L'accés a recursos es realitza, depenent de l'actiu, mitjançant elements com nom d'usuari i contrasenya, certificat, doble factor d'autenticació, targetes i/o claus.

3.2.4. Rols que requereixen separació de funcions

El rol de confiança Responsables de Seguretat no pot ser exercit per les mateixes persones que exerceixen qualsevol altre rol de confiança.

3.3. Controls de personal

El personal afectat pel que estableix aquesta secció és l' assignat als rols de confiança pel Consorci AOC i el proveïdor tecnològic.

3.3.1. Requisits de qualificació, experiència, i autorització

La TSA s' assegura que el personal designat és confiable i té la qualificació i experiència necessàries per a la prestació dels serveis oferts i, en particular, que té coneixements mínims en matèria de seguretat i gestió. L' anterior es requereix sens perjudici de la possibilitat que la TSA pugui suplir els requisits de qualificació i experiència mitjançant formació i entrenament apropiats.

3.3.2. Procediments de comprovació d' antecedents

La TSA podrà demanar certificats que acreditin la no existència d' antecedents penals per als seus empleats sempre que la norma aplicable ho permeti.

3.3.3. Requisits de formació

Per a les noves incorporacions, els responsables d' àrea o del servei en qüestió, a més de la formació tècnica específica del seu lloc, s' han d' assegurar que coneixen les practiques, les polítiques, els procediments i els requisits en matèria de seguretat de la informació i operacions del seu lloc, coneixent les conseqüències d' una desviació dels procediments establerts. Es facilitaran els documents formatius i informatius en el moment de la incorporació inicial i cada vegada que aquests es modifiquin.

Els rols de confiança Administradors de Sistemes que realitzen tasques relatives als dispositius criptogràfics (HSM) requereixen d'una formació especial en l'operació dels HSM.

3.3.4. Requisits i freqüència de l' actualització de la formació

La TSA elabora un Pla de Formació anual on es detecten les necessitats de formació del personal i es planifiquen de la forma adequada.

3.3.5. Sancions per accions no autoritzades

El procés disciplinari està especificat en el procediment intern de la TSA basat en el Reial Decret Legislatiu 2/2015, de 23 d'octubre, pel qual s'aprova el text refós de la Llei de l'Estatut dels Treballadors, que aplicarà per depurar responsabilitats derivades d'accions no autoritzades.

3.3.6. Requeriments de contractació independents

La contractació de personal a través d' una tercera empresa complirà amb els requisits establerts en aquesta DP i en els procediments interns del proveïdor tecnològic. El Consorci AOC és responsable, en tot cas, de l' efectiva execució.

Aquests aspectes queden concretats en l' instrument jurídic utilitzat per acordar la prestació dels serveis pel tercer diferent del proveïdor tecnològic.

3.3.7. Documentació proporcionada al personal

La TSA subministrarà al personal la documentació general dels serveis i específica del lloc de treball a exercir (manuals d'operació, procediments tècnics o de programació, procediments de suport, etc.) per tal que pugui desenvolupar de forma competent les seves funcions.

4. Legislació aplicable

El Consorci AOC estableix en els seus instruments jurídics amb els seus subscriptors i verificadors que la llei aplicable a la prestació del servei és la següent:

- Llei 29/2010, del 3 d'agost, d'ús dels mitjans eletrònics al sector públic de Catalunya.
- Llei 26/2010, del 3 d'agost, de règim jurídic i procediment de les administracions públiques de Catalunya.
- Reglament (UE) nº 910/2014 del Parlament Europeu i del Consell, de 23 de juliol de 2014, relatiu a la identificació electrònica i els serveis de confiança per a les transaccions electròniques en el mercat interior i per la qual es deroga la Directiva 1999/93/CE.
- Reglament (UE) 2024/1183 de Parlament Europeu i del Consell d'11 d'abril del 2024 pel qual es modifica el Reglament (UE) núm. 910/2014 pel que fa a l'establiment del marc europeu d'identitat digital
- Reglament d'Execució (UE) 2025/1929 de la Comissió de 29 de setembre de 2025 pel qual s'estableixen disposicions d'aplicació del Reglament (UE) 910/2014 del Parlament Europeu i del Consell pel que fa a la vinculació de la data i l'hora amb les dades i a l'establiment de l'exactitud de les fonts d'informació temporal pel suministrament de segells qualificats de temps electrònics
- Llei 6/2020, de l'11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança.
- Llei 39/2015, de l'1 d'octubre, del Procediment Administratiu Comú de les Administracions Públiques.
- Llei 40/2015, d'1 d'octubre, de Règim Jurídic del Sector Públic.
- Reial Decret 203/2021, de 30 de març, pel qual s'aprova el Reglament d'actuació i funcionament del sector públic per mitjans electrònics.
- Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (RGPD).
- Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals (LOPDGDD).
- Directiva (UE) 2015/2366 del Parlament Europeu i del Consell de 25 de novembre de 2015 sobre serveis de pagament en el mercat interior i per la qual es modifiquen les Directives 2002/65/CE, 2009/110/CE i 2013/36/UE i el Reglament (UE) nº 1093/2010 i es deroga la Directiva 2007/64/CE.
- Reglament d'Execució (UE) 2015/1502 de la Comissió de 8 de setembre de 2015 sobre la fixació d'especificacions i procediments tècnics mínims per als nivells de seguretat de mitjans d'identificació electrònica d'acord amb el que disposa l'article 8, apartat 3, del Reglament (UE) nº 910/2014 del Parlament Europeu i del Consell, relatiu a la identificació electrònica i els serveis de confiança per a les transaccions electròniques en el mercat interior.
- Decisió d'Execució (UE) 2016/650 de la Comissió, de 25 d'abril de 2016, per la qual es fixen les normes per a l'avaluació de la seguretat dels dispositius qualificats de creació de signatures i segells d'acord amb l'article 30, apartat 3, i a l'article 39, apartat 2, del Reglament (UE) nº 910/2014 del Parlament Europeu i del Consell, relatiu a la identificació

electrònica i els serveis de confiança per a les transaccions electròniques en el mercat interior.

- Reglament Delegat (UE) 2018/389 de la Comissió de 27 de novembre de 2017 pel qual es complementa la Directiva (UE) 2015/2366 del Parlament Europeu i del Consell pel que fa a les normes tècniques de regulació per a l'autenticació reforçada de clients i uns estàndards de comunicació oberts comuns i segur.
- Reial Decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat.
- El Marc Normatiu de Seguretat de la Informació de l'Agència de Ciberseguretat de Catalunya en l'àmbit de la Generalitat de Catalunya que determina les línies estratègiques, polítiques, estàndards i guies de seguretat pròpies de la Generalitat de Catalunya, amb caràcter supletori a falta d'un de propi.
- Política de Seguretat del Consorci AOC.

5. Resta de requisits

En el que no està especificat en aquest document, els serveis de segellat de temps sota aquesta DP es regeixen per l'especificat en els documents "Declaració de Pràctiques de Certificació (DPC) Autoritat de Certificació del Consorci AOC", "Política de Certificació per a Dispositius i Infraestructures Consorci AOC" i "Descripció dels perfils de Certificats Consorci AOC" publicats a la pàgina web https://epscd.aoc.cat/ca/index.html#politiques, en el que no sigui aplicable exclusivament als serveis d'expedició de certificats del Consorci AOC, i en el que sigui aplicable als certificats dels serveis de segellat de temps del Consorci AOC (veure OID polítiques de certificats en punt 1.2).