



**Administració
Oberta de
Catalunya**

Clàusules de Divulgació del Servei de segellat qualificat de temps



Localret

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	Clàusules de Divulgació del Servei de segellat qualificat de temps
Fitxer	Clàusula de divulgació TSA1-1.0-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	Aquesta obra està subjecta a una llicència Reconeixement - No comercial- Sense obres derivades 3.0 Espanya de Creative Commons. Per veure una còpia, visiteu http://creativecommons.org/licenses/by-nc-sa/3.0/deed.ca o envii una carta a Creative Commons, 171 Second Street, Suite 300, San Francisco, Califòrnia 94105, USA. 

Control de versions

Data:	18/12/2024
Descripció:	Versió inicial

Índex

1. Acord íntegre	4
2. Informació de contacte TSA	4
3. Tipus de certificats, i ús dels segells electrònics de temps	4
4. Sincronització de temps	5
5. Obligacions de la TSA	5
6. Obligacions dels subscriptors	5
7. Obligacions del Tercer que confia	6
8. Validació del segell de temps	6
9. Limitació i exclusió de responsabilitat	7
10. Acords aplicables i declaració de pràctiques	7
11. Política de privacitat	8
12. Política de reemborsament	8
13. Llei aplicable, reclamacions i resolució de conflictes	8
13.1. Legislació aplicable	8
13.2. Resolució extrajudicial de conflictes	8
13.3. Jurisdicció competent	8
14. TSA i dipòsit de llicències, marques de confiança i auditoria	9

1. Acord íntegre

Aquestes clàusules de divulgació són un extracte dels acords establerts per la Declaració de Pràctiques del segell qualificat de temps (en endavant **DP**) prestats pel Consorci Administració Oberta de Catalunya (en endavant, **ConSORCI AOC**), disponible en <https://tsa.aoc.cat/regulacio/>.

2. Informació de contacte TSA

El Responsable del Servei de segellat Qualificat de Temps del Consorci AOC és responsable del desenvolupament, implementació i publicació de la DP de segellat qualificat de temps del Consorci AOC, així com dels documents rellevants relacionats amb la prestació del servei de segellat de temps. Totes les consultes i comentaris relatius al contingut d'aquests documents poden adreçar-se a:

ConSORCI Administració Oberta de Catalunya

Adreça: C/ Salvador Espriu, 45.

CP: 08908

L'Hospitalet del Llobregat

e-mail: suport@aoc.cat

Telefón: (+34) 93 272 40 00

3. Tipus de certificats, i ús dels segells electrònics de temps

Els certificats de TSU de la (o les) Unitats de segellat de Temps (en endavant **TSU**, *Time Stamping Units*) operades per l'Autoritat de segellat de Temps (en endavant **TSA**, *Time-Stamping Authority*) són certificats qualificats d'acord amb l'article i Annex III del Reglament (UE) 910/2014 del Parlament Europeu i del Consell, de 23 de juliol de 2014 i compleixen amb el que disposen les normatives tècniques ETSI EN 319 411-2, ETSI EN 319 412-3, ETSI EN 319 421 i ETSI EN 319 422.

Amb aquests certificats qualificats de TSU, el Consorci AOC ofereix sota aquest document un tipus de segells de temps:

- Segells de temps qualificat

Aquest servei té com a identificador de política (OID) 0.4.0.2023.1.1, que correspon a la Política BTSP (*Best practices Time-Stamp Policy*) definit en la norma ETSI EN 319 421.

Els segells de temps electrònic declarats com a qualificats segueixen les indicacions del Reglament UE 910/2014 i el certificat de la TSU és expedit sota la política declarada en ETSI EN 319 411-2.

Els nostres segells de temps s'emeten en el format definit en els estàndards RFC 3161 i poden ser utilitzats per a qualsevol propòsit que requereixi garantir de l'existència d'un determinat resum criptogràfic en un moment determinat del temps.

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.

El Consorci AOC no guarda còpia dels segells de temps que emet. Aquests seran vàlids fins a la data de caducitat del certificat del certificat.

Els clients que reben els serveis de segellat de temps hauran d'efectuar les operacions de validació tal com preveu la **clàusula 8** i tenir en compte les limitacions i exclusions de la **clàusula 9**.

4. Sincronització de temps

La precisió declarada de l'hora en els segells de temps amb l'hora UTC és d'1 segon respecte a l'hora oficial UTC.

Veure secció 2.8 de la DP de segellat qualificat de temps per a més informació.

5. Obligacions de la TSA

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

- a) Prestar els serveis i emetre els segells de temps d'acord amb la DP.
- b) Totes les que es derivin del contingut d'aquest document, 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.

Veure punt 1.4.1 de la DP de segellat qualificat de temps per a més informació.

6. Obligacions dels subscriptors

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

- a) Utilitzar el servei d'acord amb la DP.
- b) 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.

- c) Validar els segells de temps continguts en les respostes del servei en el moment de recepció de les respostes conforme a l'especificat en la **clàusula 8**.
- d) Informar immediatament la TSA sobre qualsevol incident o fet que afecti el servei prestat o que pugui afectar la validesa dels segells de temps.
- e) Utilitzar el Servei conforme a la Llei i a les limitacions fixats en la **clàusula 9** d'aquesta Clàusula de Divulgació i en les Condicions General de prestació dels Serveis AOC publicades en: <https://web.aoc.cat/blog/serveis/condicions-prestacio-serveis-aoc/>

Veure secció 1.4.3 de la DP de segellat qualificat de temps per a més informació.

7. Obligacions del Tercer que confia

Les obligacions del Tercer que confia (també anomenat "les Parts usuaris") en un segell de temps emès per un servei de segellat de temps sota aquesta DP són:

- a) Validar el segell de temps conforme a l'especificat en la **clàusula 8**, 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).
 - Com a verificador, si el 'Tercer que confia' confia en una signatura electrònica corresponent a un segell de temps electrònic no verificada, assumirà tots els riscos i conseqüències d'aquesta actuació.
- b) Tenir en compte les limitacions d'ús especificades en la **clàusula 9**.
 - Fer un ús correcte i conforme a les lleis de la informació d'estat dels segells de temps electrònics i no comprometre la seguretat dels serveis públics de segellat de temps de Consorci AOC.

Veure Secció 1.4.4 de la DP de segellat qualificat de temps per a més informació.

8. 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 en 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 segellats.
- La signatura digital del segell de temps és correcta.
- La clau privada de la TSU usada no ha estat compromesa abans del moment de la validació del segell de temps.

- Els algorismes de hash utilitzats (en el hash de les dades segellats i en la signatura del segell de temps), i l'algoritme i la mida de clau de la signatura 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, verificar que el certificat de la TSU ha estat emès per una Autoritat de Certificació (**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.

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

9. Limitació i exclusió de responsabilitat

El Consorci AOC respondrà a les funcions que es corresponguin conforme a la DP Segell qualificat de temps tenint en compte les següents limitacions i exclusions de responsabilitat:

- Els serveis de segellat de temps sota aquesta DP no emmagatzemen ni custodien els segells de temps emesos, però Consorci AOC mantindrà els registres d'auditoria de les peticions i respostes durant un període mínim 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, de manera que es pugui 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 ni per tractar les seves respostes, sent responsabilitat del Subscriptor o dels seus usuaris finals adaptar els seus sistemes o utilitzar programari existent al mercat per realitzar les sol·licituds i tractar les respostes. Per la qual cosa Consorci AOC no es responsabilitzarà pel correcte funcionament de les aplicacions utilitzades pel Subscriptor per a això ni per deterioraments o avaries en els equips, dades o instal·lació necessària per executar el servei per causes no directament imputables a la utilització del servei.
- Consorci AOC no serà responsable dels danys derivats de o, relacionats amb, la no execució o execució defectuosa de les obligacions a càrrec del Subscriptor, ni de la incorrecta utilització dels serveis i les claus associades per al seu ús, ni de qualsevol dany indirecte que pugui resultar de la utilització del servei, en particular, el lucre cessant, la pèrdua d'ingressos o pèrdua de dades, no donant lloc a cap tipus de dret indemnitzatori.
- El Consorci AOC no assumirà cap responsabilitat per la no execució o el retard en l'execució de qualsevol de les obligacions en virtut d'aquest contracte si tal manca d'execució o retard resultés o fos conseqüència d'un supòsit de força major, cas fortuït o, en general, qualsevol circumstància sobre la qual el Consorci AOC no pugui tenir un control raonable.
- En particular, el Consorci AOC no podrà assumir cap responsabilitat sobre les dades o continguts sobre els quals s'apliqui un segell de temps electrònic.

10. Acords aplicables i declaració de pràctiques

El Servei de segellat de temps del Consorci AOC es regula tècnicament i operativament per la DP de segellat qualificat de temps, per les seves actuacions posteriors, així com per la documentació complementària.

Tal DP de segellat qualificat de temps com la documentació d'integració es poden consultar en: <https://tsa.aoc.cat/regulacio/>

També seran d'aplicació les Condicions General de prestació dels Serveis AOC publicades a: <https://web.aoc.cat/blog/serveis/condicions-prestacio-serveis-aoc/>

En tot allò no previst en la present Clàusula de Divulgació, regirà el que disposa la DP de segellat de temps. Tanmateix, en cas de contradicció entre els termes del present document i la DP de segellat de temps, prevaldrà, en tot cas, aquesta última.

11. Política de privacitat

El Servei de segellat de temps del Consorci AOC no identifica els seus usuaris, ni les operacions que porta a terme tracten dades de caràcter personal.

12. Política de reemborsament

No aplica.

13. Llei aplicable, reclamacions i resolució de conflictes

13.1. Legislació aplicable

Les parts es regiran per les lleis espanyoles, especialment per la Llei 6/2020, d'11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança i del Reglament (UE) N° 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.

13.2. Resolució extrajudicial de conflictes

La Consorci AOC estableix, en els seus instruments jurídics amb subscriptors i verificadors, els procediments de mediació i resolució de conflictes aplicables, amb l'objecte dels quals, es té en compte la seva consideració com a Administració Pública.

Les situacions de discrepància que es derivin de l'ús dels serveis de segellat de temps emesos pel Consorci AOC es resolen aplicant els mateixos criteris de competència que en els casos dels documents signats per escrit.

13.3. Jurisdicció competent

L'Autoritat de segellat de temps estableix, en els seus instruments jurídics vinculants amb subscriptors i verificadors, una clàusula de jurisdicció competent, que indica que la competència

judicial internacional correspon als jutges espanyols. La competència territorial i funcional es determina en virtut de les regles de dret internacional privat i regles de dret processal que resultin d'aplicació. Així mateix, es té en compte la legislació administrativa que resulti aplicable.

14.TSA i dipòsit de llicències, marques de confiança i auditoria

ConsortiAOC és Prestador Qualificat de Serveis de Confiança, en aplicació del Reglament UE n°910/2014 (eIDAS), havent superat les avaluacions de conformitat aplicables al Servei objecte del present document.