



**Administració
Oberta de
Catalunya**

**Política de Certificació per a
Dispositius i Infraestructures
Consorti AOC**

Referència: PC DISPOSITIUS I INFRAESTRUCTURES

Versió: 7.2

Data: 09/03/2025

OID: 1.3.6.1.4.1.15096.1.3.2.1.3

La versió original en vigor d'aquest document es troba en format electrònic publicada en el web del Consorci AOC i pot ser accessible a través de la següent URL:
<https://epscd.aoc.cat/regulacio/>

Historial de versions

Versió	Resum dels canvis	Data
5.0	Adaptació a eIDAS.	9/05/2018
6.0	Creació de nova política de certificació específica per a dispositius i infraestructures a partir de l'anterior política general. Es numera com a versió 6.0 a efectes de gestió documental per a donar continuïtat al document de política general anterior.	26/07/2018
6.1	- Revisió anual de la documentació, post auditoria eIDAS. "3.1. <i>Període de validesa dels certificats</i>": modificada validesa dels certificats d'aplicació a 4 anys. - Creat "4.3.5. <i>Validacions CAA</i>" on s'expliquen les validacions fetes sobre els registres CAA pels certificats SSL i EV.	24/07/2019
6.2	Adaptació de la Política als requeriments de la versió 2.7 de la Política de Mozilla Root Store.	31/03/2020
6.3	- Revisió de la Política. - Adequació a la Llei 6/2020, d'11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança	27/01/2021
6.4	Revisió sense canvis.	31/03/2022
6.5	Apartat 4.1.2. : actualització dades de contacte de l'organització.	29/03/2023
6.6	- Eliminades referències a QWAC y QTSA. - Canvi URLs a web epscd.aoc.cat	10/05/2023
6.7	- Apartats 3.1 i 4.3.8: Eliminació de la referencia a la suspensió de Certificats - Apartat 4.1.2: modificació per remissió a la DPC.	15/11/2023
7.0	Inclusió de la nova jerarquia AOC G3.	31/10/2024
7.1	Inclusió del Certificat de Servei de Segell Qualificat de Temps	18/12/2024
7.2	Revisió sense canvis	09/03/2025

Índex

1. Introducció	5
1.1. Presentació i àmbit d'aplicació	5
1.2. Nom del document i identificació	6
1.2.1. Identificació d'aquest document	6
1.2.2. Identificació de polítiques de certificació per a cada tipus de certificat	6
2. Entitats participants	7
2.1. Prestadors de serveis de Confiança (PSC)	7
2.2. Entitats de Registre	7
2.3. Usuaris finals	7
2.3.1. Sol·licitants de certificats	8
2.3.2. Subscriptors de certificats	8
2.3.3. Posseïdors de claus	8
2.3.4. Tercer que confia en els certificats	8
3. Característiques dels certificats	9
3.1. Període de validesa dels certificats	9
3.2. Ús dels certificats	9
3.2.1. Ús típic dels certificats	9
3.2.2. Usos prohibits	9
4. Procediments operatius	10
4.1. Administració de la Política de Certificació	10
4.1.1. Organització que administra l'especificació	10
4.1.2. Dades de contacte de l'organització	10
4.2. Publicació d'informació i directori de certificats	10
4.2.1. Directori de certificats	10
4.2.2. Publicació d'informació	10
4.3. Característiques d'operació del cicle de vida dels certificats	10
4.3.1. Sol·licitud d'emissió de certificat	10
4.3.2. Legitimació per a sol·licitar l'emissió	10
4.3.3. Processament de la sol·licitud de certificació	11
4.3.4. Generació i instal·lació de les claus d'activació	11
4.3.5. Emissió del certificat	11
4.3.6. Comunicació de l'emissió al subscriptor	12

4.3.7. Lliurament i protecció de les dades d'activació	12
4.3.8. Revocació de certificats	12
4.3.9. Renovació de certificats	12
5. Perfil dels certificats emesos sota la present Política de Certificació	13

1. Introducció

1.1. Presentació i àmbit d'aplicació

Els Certificats de dispositius i infraestructura als que es fan referència en aquesta Política de Certificació (PC) són emesos pel Consorci AOC per al seu ús per part de tots els ens que integren el sector públic de Catalunya en els termes de l'article 2.1 de la Llei 29/2010, de 3 d'agost, de l'ús dels mitjans electrònics en el sector públic de Catalunya, de conformitat amb el previst per l'art. 7 de la Llei 29/2010 i l'art. 7 dels Estatuts del Consorci AOC aprovats per Acord GOV/43/2015, de 24 de març, pel qual s'aprova la modificació dels estatuts de determinats consorcis, amb participació majoritària de la Generalitat de Catalunya.

Els Certificats de dispositius i infraestructura estan caracteritzats pel fet que el posseïdor de la clau privada és un dispositiu informàtic que realitza les operacions de signatura i desxifrat de forma automàtica, sota la responsabilitat d'una persona física o jurídica (denominat subscriptor o titular del certificat).

La present PC ha estat elaborada seguint l'estàndard RFC 3647 del IETF i els certificats emesos a l'empara de la mateixa compleixen amb els requisits establerts en l'annex I del Reglament (UE) 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 que es deroga la Directiva 1999/93/CE (Reglament (UE) núm. 910/2014).

Aquest document detalla la Política de Certificació per als següents tipus de certificats:

- Certificat d'Aplicació (Dispositiu aplicació)
- Certificat de Segell Electrònic Avançat (Segell nivell mig)
- Certificat de Servei de Segell Qualificat de Temps

Aquesta PC està subjecte al compliment de la Declaració de Pràctiques de Certificació del Consorci AOC (DPC), la qual s'hi fa referència.

1.2. Nom del document i identificació

1.2.1. Identificació d'aquest document

Nom:	PC de Dispositius i Infraestructures
Versió:	7.2
Descripció	Política de Certificació per a Dispositius i Infraestructures
Data d'emissió:	09/03/2025
OID:	1.3.6.1.4.1.15096.1.3.2.1.3
Localització:	https://epscd.aoc.cat/regulacio

1.2.2. Identificació de polítiques de certificació per a cada tipus de certificat

Tipus de certificat	OID
Certificat d'Aplicació (Dispositiu aplicació)	1.3.6.1.4.1.15096.1.3.2.91.1
Certificat de Segell Electrònic Avançat (Segell nivell mig)	1.3.6.1.4.1.15096.1.3.2.6.2
Certificat de Servei de Segell Qualificat de Temps	1.3.6.1.4.1.15096.1.3.2.112

Els documents descriptius d'aquests perfils de certificats es publiquen al web del Consorci AOC.

2. Entitats participants

2.1. Prestadors de serveis de Confiança (PSC)

Els certificats emesos a l'empara d'aquesta Política de Certificació són emesos pel Consorci AOC com a prestador de serveis de confiança a través de les seves Entitats de Certificació (d'ara endavant, EC) subordinada EC-SECTORPUBLIC, SubCA SECTOR PUBLIC Q (G3) A.1. i SubCA Q TSA (G3) A.5.

El nom comercial amb el que el Consorci AOC ofereix aquest servei és T-CAT. En aquest document, s'utilitzarà per referir-se al servei ofert pel Consorci AOC en aquest àmbit.

2.2. Entitats de Registre

Les Entitats de Registre són les persones físiques o jurídiques que assisteixen als PSC en determinats procediments i relacions amb els sol·licitants i subscriptors de certificats, especialment als tràmits d'identificació, registre i autenticació dels subscriptors dels certificats i dels posseïdors de claus.

El Consorci AOC és responsable del procés de creació d'Entitats de Registre T-CAT: verifica que l'Entitat de Registre compta amb els recursos materials i humans necessaris; i que ha designat i ha format al personal que serà responsable de l'emissió de certificats (els anomenats operadors de l'Entitat de Registre).

Existeixen els següents tipus d'Entitats de Registre T-CAT:

1. Els ens subscriptors, operats per una entitat subscriptora de certificats
2. Les Entitats de Registre, que col·laboren amb el Consorci AOC en el procés d'emissió dels certificats

Per ser Entitats de Registre, les entitats hauran de dissenyar i implantar els corresponents components i procediments tècnics, jurídics i de seguretat, referents al cicle de vida dels dispositius qualificats de creació de signatura o, si escau, de xifrat, al cicle de vida de les claus en suport programari i al cicle de vida dels certificats que emetin. Aquests components i procediments seran prèviament aprovats pel Consorci AOC.

2.3. Usuaris finals

Els usuaris finals són les persones que obtenen i utilitzen els certificats electrònics. En concret, es poden distingir els usuaris finals següents:

- Els sol·licitants de certificats.
- Els subscriptors de certificats.
- Els posseïdors de claus.
- Tercer que confia en els certificats.

2.3.1. Sol·licitants de certificats

Poden ser sol·licitants de certificats T-CAT:

- a) De certificats corporatius: una persona autoritzada a aquest efecte per la futura entitat subscriptora
- b) Una persona autoritzada pel PSC – típicament, el Consorci AOC actuant d'ofici.

L'autorització es formalitzarà documentalment.

2.3.2. Subscriptors de certificats

Els subscriptors dels certificats són les institucions i les persones, físiques o jurídiques, a nom de les quals s'emet el corresponent certificat i que s'identifiquen en el camp "Subject" del mateix.

2.3.3. Posseïdors de claus

Els posseïdors de claus són les persones físiques que posseeixen de forma exclusiva les claus d'autenticació o segellat digital de certificats, ja sigui actuant en el seu propi nom i dret, o bé, mitjançant autorització del subscriptor

Correspon al posseïdor de claus la custòdia de les dades de creació de signatura o autenticació associats al certificat digital, responsabilitzant-se el Subscriptor de qualsevol actuació realitzada pel Posseïdor de les claus.

2.3.4. Tercer que confia en els certificats

S'entén per tercer que confia en els certificats (en anglès, relying party) a tota persona o organització que voluntàriament confia en un certificat emès sota alguna de les jerarquies de certificació del Consorci AOC exposades a la Declaració de Pràctiques de Certificació.

Les obligacions i responsabilitats del Consorci AOC amb tercers que voluntàriament confiïn en els certificats es limitaran a les recollides en aquesta PC, en la DPC, en el Reglament (UE) núm. 910/2014 i en la resta de normativa que resulti d'aplicació.

Els tercers que confiïn en aquests certificats han de tenir present les limitacions en el seu ús.

3. Característiques dels certificats

3.1. Període de validesa dels certificats

Els següents certificats digitals emesos a l'empara d'aquesta Política de Certificació tindran una validesa des de la data de la seva emissió, sempre que els mateixos no resultin revocats:

- Certificat d'Aplicació (Dispositiu aplicació) : 4 anys
- Certificat de Segell Electrònic Avançat (Segell nivell mig) : 3 anys
- Certificat de Servei de Segell Qualificat de Temps: 5 anys

3.2. Ús dels certificats

Aquesta secció llista les aplicacions per les quals es pot utilitzar cada tipus de certificat, establint limitacions, i prohibeix algunes aplicacions dels certificats.

3.2.1. Ús típic dels certificats

Els certificats del Consorci AOC emesos a l'empara d'aquesta Política de Certificació podran usar-se per a les següents finalitats:

Tipus de Certificat	Àmbit d'aplicació
Certificat d'Aplicació (Dispositiu aplicació)	• Autenticació • Segellat Electrònic
Certificat de Segell Electrònic Avançat (Segell nivell mig)	• Autenticació • Segellat Electrònic
Certificat de Servei de Segell Qualificat de Temps	• Segellat de temps

3.2.2. Usos prohibits

Els certificats només es podran utilitzar dins dels límits d'ús recollits d'una manera expressa en aquesta Política de Certificació i en la DPC. Qualsevol altre ús fora dels descrits en els esmentats documents, queda exclòs expressament de l'àmbit contractual i prohibits formalment. Queda expressament prohibit qualsevol ús que sigui contrari a la Llei.

Els certificats no s'han dissenyat, no es poden destinar i no s'autoritza el seu ús o revenda com a equips de control de situacions perilloses o per a usos que requereixen actuacions a prova d'errors, com el funcionament d'instal·lacions nuclears, sistemes de navegació o comunicacions aèries, o sistemes de control d'armament, on un error podria directament comportar la mort, lesions personals o danys mediambientals severos.

Els certificats d'usuari final no poden emprar-se per signar certificats de clau pública de cap tipus, ni signar llistes de revocació de certificats.

No es recomana el seu ús per al xifrat de documents.

4. Procediments operatius

4.1. Administració de la Política de Certificació

4.1.1. Organització que administra l'especificació

ConSORCI Administració Oberta de Catalunya – Consorci AOC

4.1.2. Dades de contacte de l'organització

Segons es detalla en la DPC.

4.2. Publicació d'informació i directori de certificats

4.2.1. Directori de certificats

El servei de directori de certificats està disponible durant les 24 hores dels 7 dies de la setmana i, en cas d'error del sistema fora de control del Consorci AOC, aquesta última realitza els seus millors esforços perquè el servei es troba disponible de nou en el termini establert a la secció 5.7.4 de la DPC.

4.2.2. Publicació d'informació

La present Política de Certificació és pública i es troba disponible en el web del Consorci AOC (<https://epsd.aoc.cat/regulacio/>).

4.3. Característiques d'operació del cicle de vida dels certificats

4.3.1. Sol·licitud d'emissió de certificat

Les entitats públiques que desitgin obtenir un certificat a l'empara d'aquesta Política de Certificació poden sol·licitar-ho seguint el procediment establert en el Manual de la Carpeta del Subscriptor (<https://epsd.aoc.cat/>).

4.3.2. Legitimació per a sol·licitar l'emissió

Únicament poden sol·licitar certificats de dispositius i infraestructures les Administracions Públiques per a l'exercici de les seves funcions en l'àmbit electrònic d'acord amb la regulació que els resulti d'aplicació.

4.3.3. Processament de la sol·licitud de certificació

Quan rep una petició de certificat, l'Entitat de Certificació ha de verificar la informació proporcionada, conforme a la secció corresponent d'aquesta PC o de la DPC.

Si la informació no és correcta, l'Entitat de Certificació ha de denegar la petició. En cas contrari, l'Entitat de Certificació aprovarà la generació de certificat.

L'Entitat de Certificació haurà de:

- Utilitzar un procediment de generació de certificats que vinculi de forma segura el certificat amb la informació de registre, incloent la clau pública certificada.
- En cas que l'Entitat de Certificació generi el parell de claus, utilitzar un procediment de generació de certificats vinculat de forma segura amb el procediment de generació de claus, i que la clau privada sigui lliurada de forma segura al posseïdor de claus.
- Protegir la integritat de les dades de registre.
- Incloure en el certificat les informacions requerides.
- Garantir la data i hora en la qual es va expedir un certificat.
- Utilitzar sistemes i productes fiables que estiguin protegits contra tota alteració i que garanteixin la seguretat tècnica i, si escau, criptogràfica dels processos de certificació als quals serveixen de suport.
- Assegurar-se que el certificat és emès per sistemes que utilitzin protecció contra falsificació i, en cas que l'Entitat de Certificació generi claus privades, que garanteixin el secret de les claus durant el procés de generació d'aquestes claus.

Nota: Els procediments establerts en aquesta secció també s'apliquen en cas de renovació de certificats, ja que la renovació implica l'emissió d'un nou certificat.

4.3.4. Generació i instal·lació de les claus d'activació

L'Operador de l'Entitat de Registre validarà la veracitat i exactitud de les dades del signant comunicant-ho a l'Entitat de Certificació

L'Operador de l'Entitat de Registre validarà la possessió per part del posseïdor de claus de la clau privada associada a l'emissió del certificat electrònic.

El Consorci AOC facilita al subscriptor, d'una banda, les dades d'activació del dispositiu de creació de signatura o autenticació i, d'altra banda, al cap de 3 (tres) dies, l'accés al propi dispositiu.

4.3.5. Emissió del certificat

L'Operador de l'Entitat de Registre generarà la petició de certificat en un format estàndard i l'enviarà a l'Entitat de Certificació.

L'Entitat de Certificació validarà la integritat de la petició i que ha estat generada per un Operador de l'Entitat de Registre autoritzat. Després d'aquesta validació es procedirà a l'emissió del certificat.

4.3.6. Comunicació de l'emissió al subscriptor

El Consorci AOC comunicarà al sol·licitant l'aprovació o denegació de la sol·licitud de certificat cursada.

En cas que hagi estat aprovada, també comunicarà – quan correspongui - al futur posseïdor de claus, per correu electrònic, que s'ha generat el certificat, que es troba disponible i la forma d'obtenir-ho.

Per obtenir el certificat, el subscriptor ha d'accedir a la pàgina web que s'indica en el correu electrònic esmentat i seguir les instruccions que aquesta detalla per descarregar el certificat.

4.3.7. Lliurament i protecció de les dades d'activació

Per protegir al màxim les dades d'activació el Consorci AOC s'encarrega de distribuir els elements dels certificats per dos canals diferents.

- En primer lloc, el responsable de l'Entitat de Registre donarà accés al posseïdor de claus el següent material:
 - Full de lliurament de posseïdor
 - Dispositiu amb els certificats, en el seu cas o certificats en software
 - Software necessari per utilitzar el dispositiu
 - Carta de lliurament de certificats.
- Al mateix temps, i per correu electrònic, s'envien al posseïdor de claus les dades d'activació del certificat.

D'aquesta forma s'aconsegueix que les dades d'activació estiguin distribuïts separatament de la targeta i també en el temps.

4.3.8. Revocació de certificats

Segons es detalla en la DPC.

4.3.9. Renovació de certificats

Segons es detalla en la DPC.

5. Perfil dels certificats emesos sota la present Política de Certificació

A l'empara d'aquesta Política de Certificació s'emeten els següents tipus de certificats:

Tipus de Certificat	OID
Certificat d'Aplicació (Dispositiu aplicació)	1.3.6.1.4.1.15096.1.3.2.91.1
Certificat de Segell Electrònic Avançat (Segell nivell mig)	1.3.6.1.4.1.15096.1.3.2.6.2
Certificat de Servei de Segell Qualificat de Temps	1.3.6.1.4.1.15096.1.3.2.112

Els documents descriptius d'aquests perfils de certificats es publiquen al web del Consorci AOC (<https://epsd.aoc.cat/regulacio>).