Consorci
Administració Oberta
de Catalunya

Política de Certificació per a Certificats Personals del Sector Públic Consorci AOC

Referència:	PC CERTIFICATS PERSONALS SECTOR PÚBLIC
Versió:	6.2
Data:	31/03/2020
OID:	1.3.6.1.4.1.15096.1.3.2.1.2

La versió original en vigor d'aquest document es troba en format electrònic publicada a la web del Consorci AOC i és accessible a través de la següent URL: https://www.aoc.cat/

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 certificats personals del sector públic a partir de l'anterior política general. Es numera com a versió 6.0 a efectes de gestió documental per donar continuïtat al document de política general anterior.	26/07/2018
6.1	● Revisió anual de la documentació, post auditoria eIDAS.	24/07/2019
6.2	● Revisió anual de la documentació	31/03/2020

Índex

1. Introducció

1.1. Presentació i àmbit d'aplicació

Els Certificats electrònics a què es fa referència en aquesta Política de Certificació (PC) són emesos pel Consorci AOC per al seu ús per part de empleats públics dels 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 al 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, i persones vinculades.

La present PC ha estat elaborada utilitzant l'estàndard RFC 3647 del IETF, i els certificats emesos a l'empara de la mateixa compleixen amb els requisits establerts al Reglament (UE) 910/2014.

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

- Certificat d'autenticació de empleat públic de nivell alt (T-CAT autenticació).
- Certificat qualificat de signatura de empleat públic de nivell alt (T-CAT signatura).
- Certificat qualificat d'autenticació i signatura de empleat públic de nivell mitjà (T-CATP).
- Certificat d'autenticació de empleat públic amb pseudònim de nivell alt (T-CAT pseudònim autenticació).
- Certificat qualificat de signatura de empleat públic amb pseudònim de nivell alt (T-CAT pseudònim signatura).
- Certificat qualificat d'autenticació i signatura de persona vinculada de nivell alt (T-CAT persona vinculada).
- Certificat qualificat d'autenticació i signatura de persona vinculada de nivell mitjà (T-CATP persona vinculada).
- Certificat qualificat d'autenticació i signatura de representant davant les Administracions Públiques (T-CAT Representant).

Aquesta Política de Certificació està subjecta 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 Certificats Personals Sector Públic
Versió:	6.2
Descripció	Política de Certificació per a Certificats Personals del Sector Públic

Data d'emissió:	31/03/2020
OID:	1.3.6.1.4.1.15096.1.3.2.1.2
Localització:	https://www.aoc.cat/catcert/regulacio/

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

Tipus de certificat	OID
Certificat d'autenticació de empleat públic de nivell alt (T-CAT autenticació)	1.3.6.1.4.1.15096.1.3.2.7.1.2
Certificat qualificat de signatura de empleat públic de nivell alt (T-CAT signatura)	1. 3.6.1.4.1.15096.1.3.2.7.1.1
Certificat qualificat d'autenticació i signatura de empleat públic de nivell mitjà (T-CATP)	1.3.6.1.4.1.15096.1.3.2.7.3.1
Certificat d'autenticació de empleat públic amb pseudònim de nivell alt (T-CAT pseudònim autenticació)	1.6.1.4.1.15096.1.3.2.4.1.23
Certificat qualificat de signatura de empleat públic amb pseudònim de nivell alt (T-CAT pseudònim signatura)	1.3.6.1.4.1.15096.1.3.2.4.1.1
Certificat qualificat d'autenticació i signatura de persona vinculada de nivell alt (T-CAT persona vinculada)	1.3.6.1.4.1.15096.1.3.2.82.1
Certificat qualificat d'autenticació i signatura de persona vinculada de nivell mitjà (T-CATP persona vinculada)	1.3.6.1.4.1.15096.1.3.2.86.1
Certificat qualificat d'autenticació i signatura de representant davant les Administracions Públiques (T-CAT representant)	1.3.6.1.4.1.15096.1.3.2.8.1.1

Els documents descriptius d'aquests perfils de certificats es publiquen a la 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 la seva Entitat de Certificació (en endavant, EC) subordinada EC-SECTORPUBLIC.

2.2. Entitats de Registre

Les Entitats de Registre són les persones físiques o jurídiques que assisteixen al PSC en determinats procediments i relacions amb els sol·licitants i subscriptors de certificats,

especialment als tràmits de 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 de EC-SECTORPUBLIC. 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 d'EC-SECTORPUBLIC:

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

Per a 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 segurs de creació de signatura o, si escau, de xifrat, al cicle de vida de les claus en suport software 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 signants o posseïdors de claus.
- El tercer que confia en els certificats.

2.3.1. Sol·licitants de certificats

Poden ser sol·licitants de certificats d'EC-SECTORPUBLIC:

a) De certificats corporatius: una persona autoritzada a l'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, que s'identifiquen en el camp "Subject" del mateix.

2.3.3. Posseïdors de claus o signatàries

Els posseïdors de claus o signatàries són les persones físiques que posseeixen de forma exclusiva les claus de signatura o autenticació digital de certificats, ja sigui actuant en el seu propi nom i dret, o bé, mitjançant autorització del subscriptor, estant degudament identificades en el certificat mitjançant el seu nom i cognoms o mitjançant un pseudònim.

Correspon al signatari o posseïdor de claus la custòdia de les dades de creació de signatura o autenticació associats al certificat digital.

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 confien en els certificats es limitaran a les recollides en aquesta PC, en la DPC, en el Reglament UE 910/2014 i en la resta de normativa que resulti d'aplicació.

Els tercers que confien 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 certificats digitals emesos a l'empara d'aquesta Política de Certificació tindran una validesa de fins a 5 (cinc) anys des de la data de la seva emissió, sempre que els mateixos no resultin suspesos o revocats.

3.2. Dispositius de creació de signatura

Els següents certificats, emesos a l'empara d'aquesta Política de Certificació, utilitzen un dispositiu qualificat de creació de signatura en compliment dels requisits establerts en l'Annex II del Reglament UE 910/2014:

- Certificats qualificats d'autenticació i de signatura de empleat públic de nivell alt (T-CAT autenticació i T-CAT signatura).
- Certificats qualificats d'autenticació i de signatura de empleat públic amb pseudònim de nivell alt (T-CAT pseudònim autenticació i T-CAT pseudònim signatura).
- Certificat qualificat d'autenticació i signatura de persona vinculada de nivell alt (T-CAT persona vinculada).
- Certificat qualificat d'autenticació i signatura de representant davant les Administracions Públiques (T-CAT Representant).

La resta de certificats emesos en el marc d'aquesta Política de Certificació s'emeten en software.

3.3. 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.

3.3.1. Ús típic dels certificats

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

Tipus de Certificat	**Àmbit d'aplicació**
Certificat d'autenticació de empleat públic de nivell alt (T-CAT autenticació)	● Autenticació personal i d'atributs
Certificat qualificat de signatura de empleat públic de nivell alt (T-CAT signatura)	● Signatura electrònica
Certificat qualificat d'autenticació i signatura de empleat públic de nivell mitjà (T-CATP)	● Autenticació personal i d'atributs ● Signatura electrònica
Certificat d'autenticació de empleat públic amb pseudònim de nivell alt (T-CAT pseudònim autenticació)	● Autenticació personal i d'atributs
Certificat qualificat de signatura de empleat públic amb pseudònim de nivell alt (T-CAT pseudònim signatura)	● Signatura electrònica
Certificat qualificat d'autenticació i signatura de persona vinculada de nivell alt (T-CAT persona vinculada)	● Autenticació personal i d'atributs ● Signatura electrònica
Certificat qualificat d'autenticació i signatura de persona vinculada de nivell mitjà (T-CATP persona vinculada)	● Autenticació personal i d'atributs ● Signatura electrònica
Certificat qualificat d'autenticació i signatura de representant davant les Administracions Públiques (T-CAT Representant)	● Autenticació personal i d'atributs ● Signatura electrònica

Els Certificats emesos sota aquesta Política poden ser utilitzats amb els següents propòsits:

- **Identificació del Signant:** El Signant pot autenticar, enfront d'una altra part, la seva identitat, demostrant l'associació de la seva clau privada amb la respectiva clau pública, continguda en el Certificat. El Signant podrà identificar-se vàlidament davant qualsevol persona mitjançant la signatura d'un e-mail o qualsevol altre tipus de dades.

- **Integritat del document signat**: La utilització del Certificat garanteix que el document signat és íntegre, és a dir, garanteix que el document no va ser alterat o modificat

després de signat pel Signant. Se certifica que el missatge rebut per la Part Usuària que confia és el mateix que va ser emès pel Signant.

- **No repudi d'origen**: Amb l'ús d'aquest Certificat també es por garantir que el Signant es compromet amb les dades associades a la signatura electrònica, generant-se una evidència suficient per demostrar l'autoria de les dades associades, i la seva integritat.

3.3.2. 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 prohibit 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 severs.

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

Consorci Administració Oberta de Catalunya – Consorci AOC

Domicili social: Via Laietana, 26 – 08003 Barcelona

Direcció postal comercial: Tànger, 98, planta baixa (22@ Edifici Interface) - 08018 Barcelona

Web del Consorci AOC: https://www.aoc.cat/

Web del servei de certificació digital del Consorci AOC: https://www.aoc.cat/catcert/

Servei d'Atenció a l'Usuari: 900 90 50 90, o +34 93 272 25 01 per trucades des de l'exterior de l'estat, en horari 24x7 per a la gestió de suspensions de certificats.

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 està disponible en el lloc web del Consorci AOC (https://www.aoc.cat/catcert/regulacio/).

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

4.3.1. Sol·licitud d'emissió de certificat

La sol·licitud és el primer pas que ha de fer el subscriptor per aconseguir els certificats per al seu personal.

En el cas de les Administracions Públiques, la sol·licitud s'enviarà:

- A través de les seves Entitats de Registre T-CAT
- Directament al Consorci AOC, de forma supletoria en cas que l'ens no tingui cap Entitat de Registre assignada. En aquest cas el Consorci AOC actuarà com a Entitat de Registre T-CAT

Aquesta sol·licitud requereix l'enviament d'un document amb la informació exacta i comprovada (certificada) de les persones, entitats o dispositius per les quals es demana el certificat. Aquesta ha d'anar signada per la persona autoritzada a aquest efecte per l'entitat subscriptora, i ha de portar adjunt el certificat d'aquesta informació.

També es pot confirmar una adreça física o altres dades que permetin establir contacte directe amb el futur posseïdor de claus.

Tota la documentació es lliura a l'Entitat de Registre, per mitjans electrònics. Podrà ser remesa en suport paper o mitjançant correu electrònic, excepcionalment, pels següents motius:

- Que l'entitat subscriptora, per raó de la seva naturalesa jurídica, no pugui ser usuària de l'aplicatiu informàtic usat per remetre les sol·licituds (actualment, EACAT)
- Que sigui una entitat que sol·liciti certificats digitals per primera vegada, de manera que no disposi de cap certificat digital amb el qual dur a terme la tramitació de la sol·licitud per mitjans electrònics

4.3.2. Legitimació per sol·licitar l'emissió

Abans de l'emissió i lliurament d'un certificat, ha d'existir una sol·licitud de certificat.

En el cas de certificats individuals, el sol·licitant serà el propi subscriptor qui, alhora, serà també el posseïdor de las claus privades.

En aquest cas, ha d'haver-hi un document, en suport paper o electrònic, signat per l'Entitat de Registre, que inclourà la indicació de la persona o persones a autoritzar, per part de l'Entitat de Certificació corresponent, per realitzar peticions.

Les dades de l'usuari final necessàries per realitzar la sol·licitud seran introduïdes pel sol·licitant.

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 política 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, especialment en cas que siguin intercanviats amb el suscriptor, en cas de certificats individuals o amb el tercer sol·licitant, si escau.
- 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 servissin 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 d'ER validarà la veracitat i exactitud de les dades del signant comunicant-ho a l'Entitat de Certificació.

L'Operador d'ER validarà la possessió per part del signatari de les dades de creació de signatura (clau privada) associades 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 3 (tres) dies, l'accés al propi dispositiu.

4.3.5. Emissió del certificat

L'Operador d'ER 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 ER autoritzat. Després d'aquesta validació es procedirà a l'emissió del certificat.

4.3.6. 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 del següent material:
    - Full de lliurament de posseïdor
    - Dispositiu criptogràfic o en software amb els certificats
    - 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 separadament del dispositiu i també en el temps.

4.3.7. Suspensió de certificats

Segons es detalla en la DPC.

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'autenticació de empleat públic de nivell alt (T-CAT autenticació)	1.3.6.1.4.1.15096.1.3.2.7.1.2
Certificat qualificat de signatura de empleat públic de nivell alt (T-CAT signatura)	1.3.6.1.4.1.15096.1.3.2.7.1.1
Certificat qualificat d'autenticació i signatura de empleat públic de nivell mitjà (T-CATP)	1.3.6.1.4.1.15096.1.3.2.7.3.1
Certificat d'autenticació de empleat públic amb pseudònim de nivell alt (T-CAT pseudònim autenticació)	1.3.6.1.4.1.15096.1.3.2.4.1.2
Certificat qualificat de signatura de empleat públic amb pseudònim de nivell alt (T-CAT pseudònim signatura)	1.3.6.1.4.1.15096.1.3.2.4.1.1
Certificat qualificat d'autenticació i signatura de persona vinculada de nivell alt (T-CAT persona vinculada)	1.3.6.1.4.1.15096.1.3.2.82.1
Certificat qualificat d'autenticació i signatura de persona vinculada de nivell mitjà (T-CATP persona vinculada)	1.3.6.1.4.1.15096.1.3.2.86.1
Certificat qualificat d'autenticació i signatura de representant davant les Administracions Públiques (T-CAT Representant)	1.3.6.1.4.1.15096.1.3.2.8.1.1

Els documents descriptius d'aquests perfils de certificats es publiquen a la web del Consorci AOC (https://www.aoc.cat/catcert/regulacio/).