Consorci
Administració Oberta
de Catalunya

Política de Certificació per a Certificats de Ciutadania Consorci AOC

Referència:	PC CIUTADANIA
Versió:	6.3
Data:	21/05/2020
OID:	1.3.6.1.4.1.15096.1.3.2.1.1

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/catcert/regulacio/

Historial de versions

Versió	Resum dels canvis	Data
5.0	Adaptació a eIDAS.	9/5/2018
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
6.3	● Incorporació de mesures per Estat d'Alarma del COVID-19. ● Altres canvis menors.	21/05/2020

Índex

D'acord amb el Reial decret 463/2020, de 14 de març, pel qual es declara l'Estat d'Alarma per a la gestió de la situació de crisi sanitària ocasionada pel COVID-19, segons modificació donada pel Reial decret 465/2020, de 17 de març, la Secretaria d'Estat de Digitalització i Intel·ligència Artificial ha comunicat als diferents prestadors de serveis de confiança que no s'exigirà el compliment dels terminis establerts en l'art. 13.4 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, durant el temps de vigència de l'estat d'alarma i addicionalment, els Prestadors de Servei de Confiança podran permetre la renovació de certificats utilitzant uns altres que hagin caducat a partir del 14 de març.

1. Introducció

1.1. Presentació i àmbit d'aplicació

Els Certificats electrònics als que es fan referència en aquesta Política de Certificació (PC) són certificats **qualificats** emesos pel Consorci AOC per al seu ús per part de persones físiques que necessiten relacionar-se amb les entitats que integren el sector públic de Catalunya. Es tracta, així mateix, de certificats **personals** caracteritzats pel fet que el posseïdor de la clau privada i titular del certificat és una persona física.

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 a l'annex I del Reglament (UE) 910/2014.

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

- Certificat qualificat de Ciutadà (idCAT certificat), per a la identificació electrònica i la generació i ús de "signatures electròniques avançades".

Aquesta PC 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 de Ciutadania
Versió:	6.3

Descripció	Política de Certificació per a Certificats qualificats de Ciutadania
Data d'emissió:	21/05/2020
OID:	1.3.6.1.4.1.15096.1.3.2.1.1
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 qualificat de Ciutadà (idCAT certificat)	1.3.6.1.4.1.15096.1.3.2.86.2

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

2. Entitats participants

2.1. Prestador 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 EC (Entitat de Certificació) subordinada EC-CIUTADANIA.

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 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 d'EC-CIUTADANIA: verifica que l'Entitat de Registre compte 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).

2.3. Usuaris finals

Els usuaris finals són les persones que obtenen i utilitzen els certificats electrònics personals emesos per EC-CIUTADANIA. 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 certificats.

2.3.1. Sol·licitants de certificats

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

a) Les persones físiques que, actuant en el seu propi nom, seran els futurs Subscriptors dels certificats.
b) Altres persones autoritzades amb poders suficients pels futurs Subscriptors (representants).

2.3.2. Subscriptors de certificats

Els subscriptors dels certificats són les persones físiques a nom de les quals s'emet el corresponent certificat i que s'identifiquen en el camp "Subject" del mateix. Tenen llicència d'ús del certificat.

2.3.3. Posseïdors de claus o signants

El posseïdor de claus o signant és la persona física que crea la signatura electrònica.

Als efectes de la present PC, els posseïdors de les claus o signants són els Subscriptors dels certificats, segons s'identifiquen a l'apartat anterior.

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 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 4 (quatre) anys des de la data de la seva emissió, sempre que els mateixos no resultin suspesos o revocats.

3.2. Ús dels certificats

Els certificats idCAT de signatura avançada són certificats qualificats d'acord amb allò establert a la legislació aplicable. Els certificats idCAT no funcionen necessàriament amb dispositius qualificats de creació de signatura electrònica d'acord amb la legislació aplicable. Encara que la signatura electrònica avançada no s'equipara directament a la signatura manuscrita, aquesta equiparació es pot produir en cas d'existir un contracte de signatura electrònica o d'una norma jurídica específica on quedi reflectida aquesta equiparació.

Aquesta secció llista les aplicacions per les quals es pot utilitzar el tipus de certificat al que es refereix la present PC, 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 Qualificat de Ciutadà (idCAT certificat)	● Autenticació ● 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 pot 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.

A més, els certificats emesos sota aquesta Política podran tenir els següents usos:

- **Identificació remota**, basada en la presentació de la credencial.
- **Autenticació** per mitjans electrònics davant sistemes de control d'accés.

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 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 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 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

Adreça 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 trobi 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 y es troba 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 ús personal.

Els ciutadans que vulguin obtenir un certificat idCAT poden sol·licitar-ho de dos formes:

1. a través del web del servei idCAT del Consorci AOC, prèvia personació del Sol·licitant davant alguna Entitat de Registre autoritzada (Ajuntaments, Diputacions, etc.); o
2. personant-se directament en les oficines de qualsevol de les Entitats de Registre que ofereixen aquesta possibilitat, emplenar el formulari de sol·licitud i seguir les instruccions que allà s'indiquen.

EC-CIUTADANIA, mitjançant la participació de les Entitats de Registre, s'assegura que les sol·licituds de certificats són completes, precises i estan degudament autoritzades.

Pel que fa a las sol·licituds realitzades mitjançant la personació del Sol·licitant en les oficines d'alguna Entitat de Registre, una vegada que l'operador de registre ha comprovat favorablement la identitat del sol·licitant, ha verificat la documentació acreditativa presentada per ell i aquest ha signat el document de compareixença, l'operador signa la sol·licitud autoritzant-la i la remet a EC-CIUTADANIA.

Per a les sol·licituds emplenades via web, prèviament a la personació del Sol·licitant davant d'una Entitat de Registre: si durant l'acte de personació l'operador de registre detecta un error en les dades introduïdes - al comparar-les amb la documentació identificativa que es presenta - l'operador podrà introduir els canvis que siguin necessaris, sempre que quedi constància documentada de l'origen del canvi; de tal manera que demanarà al sol·licitant que signi un document de rectificació de dades.

Pot prescindir-se de la personació en els supòsits expressament prevists en la Llei 59/2003, de 19 de desembre.

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, a la vegada, serà també el posseïdor de les claus privades.

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 es 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 par de claus, utilitzar un procediment de generació de certificats vinculats 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 que s'expedeix un certificat.
- Garantir la data i hora en la que 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 que serveixin de suport.
- Assegurar-se de que el certificat s'emet 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, posat 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 signant de les dades de creació de signatura (clau privada) associats 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 i autenticació i, per altre 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

EC-CIUTADANIA 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 detallades per descarregar el certificat.

4.3.7. Entrega 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 de creació de signatura i autenticació.

    - Software de creació de signatura i autenticació.
    - Software necessari per a 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 de la targeta i també en el temps.

4.3.8. Suspensió de certificats

Segons es detalla en la DPC.

4.3.9. Revocació de certificats

Segons es detalla en la DPC.

4.3.10. 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'emet el següent tipus de certificat:

Tipus de Certificat	**OID**
Certificat qualificat de ciutadà (idCAT certificat)	1.3.6.1.4.1.15096.1.3.2.86.2

El document descriptiu d'aquest perfil de certificat es publica en el web del Consorci AOC (https://www.aoc.cat/catcert/regulacio/).