Administració Oberta de Catalunya

Política de Certificación para Certificados de Ciudadanía Consorci AOC

Referencia:	PC CIUDADANÍA
Versión:	7.1
Fecha:	18/12/2024
OID:	1.3.6.1.4.1.15096.1.3.2.1.1

La versión original en vigor de este documento se encuentra en formato electrónico publicada en el sitio web del Consorci AOC y puede ser accesible a través de la siguiente URL: https://epscd.aoc.cat/regulacio.

Historial de versiones

Versión	Resumen de los cambios	Fecha
5.0	Adaptación a eIDAS.	9/5/2018
6.0	Creación de nueva política de certificación específica para ciudadanía a partir de la anterior política general. Se numera como versión 6.0 a efectos de gestión documental para dar continuidad al documento de política general anterior.	26/07/2018
6.1	● Revisión anual de la documentación, post auditoría eIDAS.	24/07/2019
6.2	● Revisión anual de la documentación.	31/03/2020
6.3	● Incorporación de medidas por Estado de Alarma del COVID-19 ● Otros cambios menores	21/05/2020
6.4	● Supresión de medidas por Estado de Alarma del COVID-19 ● Otros cambios menores	03/08/2020
6.5	● Adaptación a la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.	27/01/2021
6.6	● Revisión sin cambios	31/03/2022
6.7	● Apartado 4.1.2: actualización datos de contacto de la organización.	29/03/2023
6.8	● Apartado 4.3.8: Eliminación de la referencia a la suspensión de certificados. ● Apartado 4.1.2: modificación para remitir a la información en la DPC.	15/11/2023
7.0	● Inclusión de la nueva jerarquía AOC G3.	31/10/2024
7.1	● Revisión sin cambios	18/12/2024

Índice

1. Introducción

1.1. Presentación y ámbito de aplicación

Los Certificados electrónicos a los que se hace referencia en esta Política de Certificación (PC) son certificados **cualificados** emitidos por el Consorci AOC para su uso por parte de personas físicas que necesitan relacionarse con las entidades que integran el sector público de Cataluña. Se trata asimismo de certificados **personales**, caracterizados por el hecho de que el poseedor de la clave privada y titular del certificado es una persona física.

La presente PC ha sido elaborada siguiendo el estándar RFC 3647 del IETF y los certificados emitidos al amparo de la misma cumplen con los requisitos establecidos en el anexo I del Reglamento (UE) nº 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (Reglamento (UE) nº 910/2014).

Este documento detalla la Política de Certificación para los siguientes tipos de certificados:

- Certificado cualificado de Ciudadano (idCAT certificat), para la identificación electrónica y la generación y uso de “firmas electrónicas avanzadas”.

Esta PC está sujeta al cumplimiento de la Declaración de Prácticas de Certificación del Consorci AOC (DPC), a la cual se hace referencia.

1.2. Nombre del documento e identificación

1.2.1. Identificación de este documento

Nombre:	PC de Ciudadanía
Versión:	7.1
Descripción	Política de Certificación para Certificados cualificados de Ciudadanía
Fecha de emisión:	18/12/2024
OID:	1.3.6.1.4.1.15096.1.3.2.1.1
Localización:	https://epscd.aoc.cat/regulacio

1.2.2. Identificación de políticas de certificación para cada tipo de certificado

Tipo de certificado	OID
Certificado cualificado de Ciudadano (idCAT certificat)	1.3.6.1.4.1.15096.1.3.2.86.2

Los documentos descriptivos de estos perfiles de certificados se publican en el web del Consorci AOC.

2. Entidades participantes

2.1. Prestadores de servicios de confianza (PSC)

Los certificados emitidos al amparo de esta Política de Certificación son emitidos por el Consorci AOC como prestador de servicios de confianza a través de sus CA (Certification Authority, o Autoridad de Certificación) subordinada EC-CIUTADANIA y SubCA CIUTADANIA Q (G3) A.2.

El nombre comercial con el que el Consorci AOC ofrece este servicio es idCAT Certificat. En este documento, se utilizará para referirse al servicio ofrecido por el Consorcio AOC en este ámbito.

2.2. Autoridades de Registro

Las Autoridades de Registro son las personas físicas o jurídicas que asisten a los PSC en determinados procedimientos y relaciones con los solicitantes y suscriptores de certificados, especialmente a los trámites de identificación, registro y autenticación de los suscriptores de los certificados y de los poseedores de claves.

El Consorci AOC es responsable del proceso de creación de Autoridades de Registro de idCAT Certificat : verifica que la Autoridad de Registro cuenta con los recursos materiales y humanos necesarios; y que ha designado y ha formado al personal que será responsable de la emisión de certificados (los llamados operadores de la Autoridad de Registro).

2.3. Usuarios finales

Los usuarios finales son las personas que obtienen y utilizan los certificados electrónicos personales idCAT Certificat. En concreto, se pueden distinguir los usuarios finales siguientes:

- Los solicitantes de certificados.
- Los suscriptores de certificados.
- Los poseedores de claves.
- Tercero que confía en los certificados.

2.3.1. Solicitantes de certificados

Pueden ser solicitantes de certificados de idCAT Certificat

a) Las personas físicas que, actuando en su propio nombre, serán los futuros Suscriptores de los certificados.
b) Otras personas físicas que acompañen la documentación en los términos legalmente establecidos (legitimación notarial de la firma de los futuros Suscriptores).

2.3.2. Suscriptores de certificados

Los suscriptores de los certificados son las personas físicas a nombre de las cuales se emite el correspondiente certificado y que se identifican en el campo “Subject” del mismo. Tienen licencia de uso del certificado.

2.3.3. Poseedores de claves o firmantes

El poseedor de claves o firmante es la persona física que crea la firma electrónica.

A los efectos de la presente PC, los poseedores de las claves o firmantes son los Suscriptores de los certificados, según se identifican en el apartado anterior.

2.3.4. Tercero que confía en los certificados

Se entiende por tercero que confía en los certificados (en inglés, *relying party*) a toda persona u organización que voluntariamente confía en un certificado emitido bajo alguna de las jerarquías de certificación del Consorci AOC expuestas en la Declaración de Prácticas de Certificación.

Las obligaciones y responsabilidades del Consorci AOC con terceros, que voluntariamente confíen en los certificados, se limitarán a las recogidas en esta PC, en la DPC, en el Reglamento (UE) nº 910/2014 y en el resto de normativa que resulte de aplicación.

Los terceros que confíen en estos certificados deben tener presente las limitaciones en su uso.

3. Características de los certificados

3.1. Periodo de validez de los certificados

Los certificados digitales emitidos al amparo de esta Política de Certificación tendrán una validez de 4 (cuatro) años desde la fecha de su emisión, siempre que los mismos no resulten revocados.

3.2. Uso de los certificados

Los certificados idCAT de firma avanzada son certificados cualificados de acuerdo con lo establecido en la legislación aplicable. Los certificados idCAT no funcionan necesariamente con dispositivos cualificados de creación de firma electrónica de acuerdo con dicha legislación aplicable. Aunque la firma electrónica avanzada no se equipara directamente a la firma escrita, esta equiparación se puede producir en caso de existir un contrato de firma electrónica o de una norma jurídica específica donde quede reflejada esta equiparación.

Esta sección lista las aplicaciones para las que se puede utilizar el tipo de certificado al que se refiere la presente PC, estableciendo limitaciones, y prohíbe algunas aplicaciones de los certificados.

3.2.1. Uso típico de los certificados

Los certificados del Consorci AOC emitidos al amparo de esta Política de Certificación podrán usarse para los siguientes fines:

Tipo de Certificado	Ámbito de aplicación
Certificado Cualificado de Ciudadano (idCAT certificat)	● Autenticación ● Firma electrónica

Los certificados emitidos bajo esta Política pueden ser utilizados con los siguientes propósitos:

- **Identificación del Firmante:** El Firmante puede autenticar, frente a otra parte, su identidad, demostrando la asociación de su clave privada con la respectiva clave pública, contenida en el Certificado. El Firmante podrá identificarse válidamente ante cualquier persona mediante la firma de un e-mail o cualquier otro tipo de datos.

- **Integridad del documento firmado**: La utilización del Certificado garantiza que el documento firmado es íntegro, es decir, garantiza que el documento no fue alterado o modificado después de firmado por el Firmante. Se certifica que el mensaje recibido , por la Parte Usuariaque confía, es el mismo que fue emitido por el Firmante.

- **No repudio de origen**: Con el uso de este Certificado también se puede garantizar que el Firmante se compromete con los datos asociados a la firma electrónica, generándose una evidencia suficiente para demostrar la autoría de los datos asociados, y su integridad.

Además, los certificados emitidos bajo esta Política podrán tener los siguientes usos:

- **Identificación remota**, basada en la presentación de la credencial.
- **Autenticación** por medios electrónicos ante sistemas de control de acceso.

3.2.2. Usos prohibidos

Los certificados sólo se podrán utilizar dentro de los límites de uso recogidos de una manera expresa en esta Política de Certificación y en la DPC. Cualquier otro uso fuera de los descritos en los mencionados documentos, queda excluido expresamente del ámbito contractual y prohibidos formalmente. Queda expresamente prohibido cualquier uso que sea contrario a la Ley.

Los certificados no se han diseñado, no se pueden destinar y no se autoriza su uso o reventa como equipos de control de situaciones peligrosas o para usos que requieren actuaciones a prueba de errores, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas, o sistemas de control de armamento, donde un error podría directamente comportar la muerte, lesiones personales o daños medioambientales severos.

Los certificados de usuario final no pueden emplearse para firmar certificados de clave pública de ningún tipo, ni firmar listas de revocación de certificados.

No se recomienda su uso para el cifrado de documentos.

4. Procedimientos operativos

4.1. Administración de la Política de Certificación

4.1.1. Organización que administra la especificación

Consorci Administració Oberta de Catalunya – Consorci AOC

4.1.2. Datos de contacto de la organización

Según se detalla en la DPC.

4.2. Publicación de información y directorio de certificados

4.2.1. Directorio de certificados

El servicio de directorio de certificados está disponible durante las 24 horas del día, los 7 días de la semana y, en caso de error del sistema fuera de control del Consorci AOC, esta última realiza sus mejores esfuerzos porque el servicio se encuentre disponible de nuevo en el plazo establecido a la sección 5.7.4 de la DPC.

4.2.2. Publicación de información

La presente Política de Certificación es pública y se encuentra disponible en el sitio web del Consorci AOC (https://epscd.aoc.cat/regulacio).

4.3. Características de operación del ciclo de vida de los certificados

4.3.1. Solicitud de emisión de certificado

La solicitud es el primer paso que tiene que hacer el Suscriptor para conseguir los certificados para su uso personal.

Los ciudadanos que deseen obtener un certificado idCAT pueden solicitarlo de dos maneras:

1. a través de la web del servicio idCAT del Consorci AOC previa personación del Solicitante ante alguna Autoridad de Registro autorizada (Ayuntamientos, Diputaciones, etc.); o
2. personándose directamente en las oficinas de cualquiera de las Autoridades de Registro que ofrecen esta posibilidad, rellenar el formulario de solicitud y seguir las instrucciones que allá se indican.

El Consorci AOC, mediante la participación de las Autoridades de Registro, se asegura que las solicitudes de certificados son completas, precisas y están debidamente autorizadas.

En lo que respecta a las solicitudes realizadas mediante la personación del Solicitante en las oficinas de alguna Autoridad de Registro, una vez que el operador de registro ha comprobado favorablemente la identidad del solicitante ha verificado la documentación acreditativa presentada por él y este ha firmado el documento de comparecencia, el operador firma la solicitud autorizándola y la remite a la Entidad de Certificación.

Para las solicitudes rellenadas vía web, previamente a la personación del Solicitante ante una Autoridad de Registro: si durante el acto de personación el operador de registro detecta algún error en los datos introducidos – al compararlas con la documentación identificativa que se presenta – el operador podrá introducir los cambios que sean necesarios, siempre que quede constancia documentada del origen del cambio; para lo cual pedirá al solicitante que firme un documento de rectificación de datos.

Puede prescindirse de la personación en los supuestos expresamente previstos en la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

4.3.2. Legitimación para solicitar la emisión

Antes de la emisión y entrega de un certificado, ha de existir una solicitud de certificado.

En el caso de certificados individuales, el solicitante será el propio suscriptor quien, a la vez, será también el poseedor de las claves privadas.

4.3.3. Procesamiento de la solicitud de certificación

Cuando recibe una petición de certificado, la Entidad de Certificación ha de verificar la información proporcionada, conforme a la sección correspondiente de esta política o de la DPC.

Si la información no es correcta, la Entidad de Certificación ha de denegar la petición. En caso contrario, la Entidad de Certificación aprobará la generación de certificado.

La Entidad de Certificación tendrá que:

- Utilizar un procedimiento de generación de certificados que vincule de forma segura el certificado con la información de registro, incluyendo la clave pública certificada.
- En caso de que la Entidad de Certificación genere el par de claves, utilizar un procedimiento de generación de certificados vinculado de forma segura con el procedimiento de generación de claves, y que la clave privada sea entregada de forma segura al poseedor de claves.
- Proteger la integridad de los datos de registro.
- Incluir en el certificado las informaciones requeridas.
- Garantizar la fecha y hora en la que se expidió un certificado.
- Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirviesen de soporte.
- Asegurarse de que el certificado es emitido por sistemas que utilicen protección contra falsificación y, en caso de que la Entidad de Certificación genere claves privadas, que garanticen el secreto de las claves durante el proceso de generación de estas claves.

Nota: Los procedimientos establecidos en esta sección también se aplican en caso de renovación de certificados, puesto que la renovación implica la emisión de un nuevo certificado.

4.3.4. Generación e instalación de las claves de activación

El Operador de la Autoridad de Registro validará la veracidad y exactitud de los datos del firmante comunicándoselo a la Entidad de Certificación.

El operador de la Autoridad de Registro validará la posesión por parte del firmante de los datos de creación de firma (clave privada) asociados a la emisión del certificado electrónico.

El Consorci AOC facilita al Suscriptor, por un lado, los datos de activación del dispositivo de creación de firma y autenticación y, por otro lado, al cabo de 3 (tres) días, el acceso al propio dispositivo.

4.3.5. Emisión del certificado

El Operador de la Autoridad de Registro generará la petición de certificado en un formato estándar y la enviará a la Entidad de Certificación.

La Entidad de Certificación validará la integridad de la petición y que ha sido generada por un Operador de la Autoridad de Registro autorizado. Tras esta validación se procederá a la emisión del certificado.

4.3.6. Comunicación de la emisión al suscriptor

El Consorci AOC comunicará al solicitante la aprobación o denegación de la solicitud de certificado cursada.

En caso de que haya sido aprobada, también comunicará – cuando corresponda - al futuro poseedor de claves, por correo electrónico, que se ha generado el certificado, que se encuentra disponible y la forma de obtenerlo.

Para obtener el certificado, el suscriptor tiene que acceder en la página web que se indica en el correo electrónico mencionado y seguir las instrucciones que estén detalladas para descargar el certificado.

4.3.7. Entrega y protección de los datos de activación

Para proteger al máximo los datos de activación el Consorci AOC se encarga de distribuir los elementos de los certificados por dos canales diferentes.

- En primer lugar, el responsable de la Autoridad de Registro dará acceso al poseedor de claves el siguiente material:
    - Hoja de entrega de poseedor
    - Dispositivo de creación de firma y autenticación.
    - Software necesario para utilizar el dispositivo
    - Carta de entrega de certificados.
- Al mismo tiempo, y por correo electrónico, se envían al poseedor de claves los datos de activación del certificado.

De esta forma se consigue que los datos de activación estén distribuidos separadamente de la tarjeta y también en el tiempo.

4.3.8. Revocación de certificados

Según se detalla en la DPC.

4.3.9. Renovación de certificados

Según se detalla en la DPC.

5. Perfil de los certificados emitidos bajo la presente Política de Certificación

Al amparo de esta Política de Certificación se emite el siguiente tipo de certificado:

Tipo de Certificado	OID
Certificado cualificado de ciudadano (idCAT certificat)	1.3.6.1.4.1.15096.1.3.2.86.2

El documento descriptivo de este perfil de certificado se publica en el web del Consorci AOC (https://epscd.aoc.cat/regulacio).