Administració Oberta de Catalunya

Política de Certificación para Dispositivos e Infraestructuras Consorci AOC

Referencia:	PC DISPOSITIVOS E INFRAESTRUCTURAS
Versión:	7.2
Fecha:	09/03/2025
OID:	1.3.6.1.4.1.15096.1.3.2.1.3

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.	9/05/2018
6.0	● Creación de nueva política de certificación específica para dispositivos e infraestructuras 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. ● "3.1. Periodo de validez de los certificados": modificada validez de los certificados de aplicación a 4 años. ● Creado "4.3.5. Validaciones CAA" donde se explican las validaciones hechas sobre los registros CAA para los certificados SSL y EV.	24/07/2019
6.2	● Adaptación de la Política a los requerimientos de la versión 2.7 de la Política de Mozilla Root Store.	31/03/2020
6.3	● Revisión de la Política ● Adaptación a la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza	27/01/2021
6.4	● Revisión sin cambios.	31/03/2022
6.5	● Apartado 4.1.2: actualización datos de contacto de la organización.	29/03/2023
6.6	● Eliminadas referencias a QWAC y QTSA. ● Cambio URLs a web epscd.aoc.cat	10/05/2023
6.7	● Apartados 3.1 y 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. Se numera como versión 7.0 a efectos de gestión documental	31/10/2024
7.1	● Inclusión del Certificado de Servicio de Sello Cualificado de Tiempo	18/12/2024
7.2	● Revisión sin cambios	09/03/2025

Índice

1. Introducción 4
1.1. Presentación y ámbito de aplicación 4
1.2.1. Identificación de este documento 5
1.2.2. Identificación de políticas de certificación para cada tipo de certificado 5

2. Entidades participantes 6
2.1. Prestadores de servicios de confianza (PSC) 6
2.2. Autoridades de Registro 6
2.3. Usuarios finales 6
2.3.1. Solicitantes de certificados 7
2.3.2. Suscriptores de certificados 7
2.3.3. Poseedores de claves 7
2.3.4. Tercero que confía en los certificados 7

3. Características de los certificados 10
3.2. Uso de los certificados 10
3.2.1. Uso típico de los certificados 10
3.2.2. Usos prohibidos 10

4. Procedimientos operativos 11
4.1. Administración de la Política de Certificación 11
4.1.1. Organización que administra la especificación 11
4.1.2. Datos de contacto de la organización 11
4.2. Publicación de información y directorio de certificados 11
4.2.1. Directorio de certificados 11
4.2.2. Publicación de información 11
4.3. Características de operación del ciclo de vida de los certificados 11
4.3.1. Solicitud de emisión de certificado 11
4.3.2. Legitimación para solicitar la emisión 11
4.3.3. Procesamiento de la solicitud de certificación 12
4.3.4. Generación e instalación de las claves de activación 12
4.3.5. Emisión del certificado 12
4.3.6. Comunicación de la emisión al suscriptor 13
4.3.7. Entrega y protección de los datos de activación 13
4.3.8. Revocación de certificados 13
4.3.9. Renovación de certificados 13

5. Perfil de los certificados emitidos bajo la presente Política de Certificación 14

1. Introducción

1.1. Presentación y ámbito de aplicación

Los Certificados de dispositivos e infraestructura a los que se hace referencia en esta Política de Certificación (PC) son emitidos por el Consorci AOC para su uso por parte de todos los entes que integran el sector público de Cataluña en los términos del artículo 2.1 de la Ley 29/2010, de 3 de agosto, del uso de los medios electrónicos en el sector público de Cataluña, en conformidad con el previsto por el art. 7 de la Ley 29/2010 y el art. 7 de los Estatutos del Consorci AOC aprobados por Acuerdo GOV/43/2015, de 24 de marzo, por el cual se aprueba la modificación de los estatutos de determinados consorcios, con participación mayoritaria de la Generalitat de Cataluña.

Los certificados de dispositivo e infraestructura están caracterizados por el hecho que el poseedor de la clave privada es un dispositivo informático que realiza las operaciones de firma y descifrado de forma automática, bajo la responsabilidad de una persona física o jurídica (denominado suscriptor o titular del certificado).

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 de Aplicación (Dispositiu aplicació)
- Certificado de Sello Electrónico Avanzado (Segell nivell mig)
- Certificado de Servicio de Sello Cualificado de Tiempo

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

1.2. Nombre del documento e identificación

1.2.1. Identificación de este documento

Nombre:	PC de Dispositivos e Infraestructuras
Versión:	7.2
Descripción	Política de Certificación para Dispositivos e Infraestructuras
Fecha de emisión:	09/03/2025
OID:	1.3.6.1.4.1.15096.1.3.2.1.3
Localización:	https://epscd.aoc.cat/regulacio

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

Tipo de certificado	OID
Certificado de Aplicación (Dispositiu aplicació)	1.3.6.1.4.1.15096.1.3.2.91.1
Certificado de Sello Electrónico Avanzado (Segell nivell mig)	1.3.6.1.4.1.15096.1.3.2.6.2
Certificado de Servicio de Sello Cualificado de Tiempo	1.3.6.1.4.1.15096.1.3.2.112

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 Autoridades de Certificación (en adelante CA, del inglés: Certification Authority) subordinada EC-SECTORPUBLIC, SubCA SECTOR PUBLIC Q (G3) A.1 y SubCA Q TSA (G3) A.5.

El nombre comercial con el que el Consorcio AOC ofrece este servicio es T-CAT. 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 T-CAT: 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).

Existen los siguientes tipos de Autoridades de Registro de T-CAT:

1. Los entes suscriptores, operados por una entidad suscriptora de certificados
2. Las Autoridades de Registro, que colaboran con el Consorci AOC en el proceso de emisión de los certificados

Para ser Autoridades de Registro, las entidades tendrán que diseñar e implantar los correspondientes componentes y procedimientos técnicos, jurídicos y de seguridad, referentes al ciclo de vida de los dispositivos cualificados de creación de firma o, en su caso, de cifrado, al ciclo de vida de las claves en apoyo software y al ciclo de vida de los certificados que emitan. Estos componentes y procedimientos serán previamente aprobados por el Consorci AOC.

2.3. Usuarios finales

Los usuarios finales son las personas que obtienen y utilizan los certificados electrónicos. 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 T-CAT:

a) De certificados corporativos: una persona autorizada al efecto por la futura entidad suscriptora

b) Una persona autorizada por el PSC – típicamente, el Consorci AOC actuando de oficio.

La autorización se formalizará documentalmente.

2.3.2. Suscriptores de certificados

Los suscriptores de los certificados son las instituciones y las personas, físicas o jurídicas, a nombre de las cuales se emite el correspondiente certificado y que se identifican en el campo "Subject" del mismo.

Los requisitos que debe reunir un suscriptor para cada tipo de certificado regido por la presente Política de Certificación son los siguientes:

2.3.3. Poseedores de claves

Los poseedores de claves son las personas físicas que poseen de forma exclusiva las claves de autenticación o sellado digital de certificados, ya sea actuando en su propio nombre y derecho, o bien, mediante autorización del suscriptor.

Corresponde al poseedor de claves la custodia de los datos de creación de firma o autenticación asociados al certificado digital, responsabilizándose el Suscriptor de cualquier actuación realizada por el Poseedor de las claves.

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 siguientes certificados digitales emitidos al amparo de esta Política de Certificación tendrán una validez desde la fecha de su emisión, siempre que los mismos no resulten revocados:

- Certificado de Aplicación (Dispositiu aplicació): 4 años.
- Certificado de Sello Electrónico Avanzado (Segell nivell mig): 3 años.
- Certificado de Servicio de Sello Cualificado de Tiempo: 5 años

3.2. Uso de los certificados

Esta sección lista las aplicaciones para las que se puede utilizar cada tipo de certificado, 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 de Aplicación (Dispositiu aplicació)	● Autenticación ● Sellado Electrónico
Certificado de Sello Electrónico Avanzado (Segell nivell mig)	● Autenticación ● Sellado Electrónico
Certificado de Servicio de Sello Cualificado de Tiempo	● Sellado de tiempo

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 de 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

Las entidades públicas que deseen obtener un certificado al amparo de esta Política de Certificación pueden solicitarlo siguiendo el procedimiento establecido en el Manual de la Carpeta del Subscriptor (https://epscd.aoc.cat/).

4.3.2. Legitimación para solicitar la emisión

Únicamente pueden solicitar certificados de dispositivos e infraestructuras las Administraciones Públicas para el ejercicio de sus funciones en el ámbito electrónico de acuerdo con la regulación que les resulte de aplicación.

4.3.3. Procesamiento de la solicitud de certificación

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

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

La Autoridad 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 Autoridad 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 sirven de soporte.
- Asegurarse de que el certificado es emitido por sistemas que utilicen protección contra falsificación y, en caso de que la Autoridad 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 Autoridad de Certificación.

El Operador de la Autoridad de Registro validará la posesión por parte del poseedor de claves de la clave privada asociada 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 o 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 Autoridad de Certificación.

La Autoridad 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, 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 éste detalla 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 con los certificados, en su caso, o certificados en software
    - 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 emiten los siguientes tipos de certificados:

Tipo de Certificado	**OID**
Certificado de Aplicación (Dispositiu aplicació)	1.3.6.1.4.1.15096.1.3.2.91.1
Certificado de Sello Electrónico Avanzado (Segell nivell mig)	1.3.6.1.4.1.15096.1.3.2.6.2
Certificado de Servicio de Sello Cualificado de Tiempo	1.3.6.1.4.1.15096.1.3.2.112

Los documentos descriptivos de estos perfiles de certificados se publican en el web del Consorci AOC (https://epscd.aoc.cat/regulacio).