Consorci
Administració Oberta
de Catalunya

Política de Certificación para
Dispositivos e Infraestructuras
Consorci AOC

Referencia:	PC DISPOSITIVOS E INFRAESTRUCTURAS
Versión:	6.2
Fecha:	31/03/2020
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://www.aoc.cat/catcert/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

Índice

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 al sector público de Cataluña, en conformidad con el previsto por el arte. 7 de la Ley 29/2010 y el arte. 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) 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 Sede Electrónica (Seu-e nivell mig)
- Certificado de Servidor Seguro (Dispositiu SSL)
- Certificado de Servidor Seguro Extended Validation (Dispositiu SSL EV)
- Certificado de Sello Cualificado de Tiempo (Segell de temps)

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:	6.2
Descripción	Política de Certificación para Dispositivos e Infraestructuras
Fecha de emisión:	31/03/2020
OID:	1.3.6.1.4.1.15096.1.3.2.1.3
Localización:	https://www.aoc.cat/catcert/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 Sede Electrónica (Seu-e nivell mig)	1.3.6.1.4.1.15096.1.3.2.5.2
Certificado de Servidor Seguro (Dispositiu SSL)	1.3.6.1.4.1.15096.1.3.2.51.1
Certificado de Servidor Seguro Extended Validation (Dispositiu SSL EV)	1.3.6.1.4.1.15096.1.3.2.51.2
Certificado de Sello Cualificado de Tiempo (Segell de Temps)	1.3.6.1.4.1.15096.1.3.2.111

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 certificación (PSC)

Los certificados emitidos al amparo de esta Política de Certificación son emitidos por el Consorci AOC como prestador de servicios de certificación a través de su CA (Certification Authority, o Autoridad de Certificación) subordinada EC-SECTORPUBLIC.

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 EC-SECTORPUBLIC: 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 EC-SECTORPUBLIC:

1. Los entes suscriptor, operadas por una entidad suscriptora de certificados
2. Las Autoridades de Registro, que colaboran con EC-SECTORPUBLIC 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 seguros 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 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 EC-SECTORPUBLIC:

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 DPC, en el Reglamento UE 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 suspendidos o revocados:

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

El resto de certificados emitidos en el marco de esta Política de certificación tendrán una validez de 2 años desde la fecha de su emisión, siempre que los mismos no resulten suspendidos o revocados.

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 Sede Electrónica (Seu-e nivell mig)	● Autenticación ● Sellado Electrónico
Certificado de Servidor Seguro (Dispositiu SSL)	● Autenticación
Certificado de Servidor Seguro Extended Validation (Dispositiu SSL EV)	● Autenticación

Certificado de Sello Cualificado de Tiempo (Segell de Temps)	• Autenticación • Sellado Electrónico • Acreditación de fecha y hora

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. Cualquiera 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

Consorci Administració Oberta de Catalunya – Consorci AOC

Domicilio social: Via Laietana, 26 – 08003 Barcelona

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

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

Web del servicio de certificación digital del Consorci AOC:

https://www.aoc.cat/catcert/

Servicio de Atención al Usuario: 900 90 50 90, o +34 93 272 25 01 para llamadas desde el exterior del estado, en horario 24x7.

Incidentes con los certificados de autenticación web: incident_pki@aoc.cat

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://www.aoc.cat/catcert/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://www.aoc.cat/catcert/).

4.3.2. Legitimación para solicitar la emisión

Únicamente pueden solicitar certificados de dispositivos e infraestructuras las Administraciones Públicas para el ejercicio de 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 política 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 sirviesen 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 comunicandoselo 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. Validaciones Certification Authority Authorization (CAA)

Previa a la emisión de los certificados SSL OV, SSL EV y Sede, se valida la existencia de registro CAA para cada nombre DNS de las extensiones CN y subjectAltName del certificado.

La comprobación de la validación del dominio se detalla en el punto 3.2.4 de la DPC.

En el supuesto de que se emita el certificado, la validación se realizará antes del time-to-live (TTL) del registro CAA.

El Consorci AOC procesa los tags "issue" y "issuewild".

El registro CAA que identifica a dominios para los cuales se autoriza la emisión por parte del Consorci AOC es "aoc.cat".

4.3.6. 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.

4.3.7. 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 éste detalla para descargar el certificado.

4.3.8. 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
    - 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.

4.3.9. Suspensión de certificados

No está permitida la suspensión de los certificados de autenticación web. Para el resto de certificados recogidos en esta CP, según se detalla en la DPC.

4.3.10. Revocación de certificados

Según se detalla en la DPC.

4.3.11. Renovación de certificados

Según se detalla en la DPC.

4.3.12. Certificado de Sello Cualificado de Tiempo

Permite garantizar la integridad de un archivo o una comunicación electrónicos en una fecha y hora determinadas, tomando una fuente de tiempo confiable. Los Certificados de Sello Cualificado de tiempo emitidos por el Consorcio AOC cumplen con los requisitos establecidos en el artículo 42 del Reglamento UE 910/2014.

El servicio de sellado de tiempo del Consorci AOC se describe en https://www.aoc.cat y en su correspondiente política disponible también en el mismo sitio web.

4.4. Notificación de problemas con certificados de autenticación de sitio web

Para notificar cualquier problema relacionada con el uso, corrección, seguridad u otro, relativo en cualquier clase de certificado de autenticación de sitio web o certificado SSL emitido por el Consorci Administració Oberta de Catalunya, a saber:

- Certificado de Servidor Seguro (Dispositiu SSL)
- Certificado de Servidor Seguro Extended Validation (Dispositiu SSL EV)
- Certificado de Sede Electrónica (Seu-e nivell mig)

Por favor contacte con el Consorci AOC a través de los Datos de contacto de la organización o en la dirección electrónica siguiente:

incident_pki@aoc.cat,

proporcionando, si es posible:

- Fecha y hora
- Número de serie del certificado
- URL a la que se está accediendo
- dirección IP desde la que se está intentando acceder a la URL.

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 Sede Electrónica (Seu-e nivell mig)	1.3.6.1.4.1.15096.1.3.2.5.2
Certificado de Servidor Seguro (Dispositiu SSL)	1.3.6.1.4.1.15096.1.3.2.51.1
Certificado de Servidor Seguro Extended Validation (Dispositiu SSL EV)	1.3.6.1.4.1.15096.1.3.2.51.2
Certificado de Sello Cualificado de Tiempo (Segell de Temps)	1.3.6.1.4.1.15096.1.3.2.111

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