Consorci
Administració Oberta
de Catalunya

Política de Certificación para Certificados Personales del Sector Público Consorci AOC

Referencia:	PC CERTIFICADOS PERSONALES SECTOR PÚBLICO
Versión:	6.0
Fecha:	26/07/2018
OID:	1.3.6.1.4.1.15096.1.3.2.1.2

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/

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 certificados personales del sector público 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

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 emitidos por el Consorci AOC para su uso por parte de trabajadores públicos y personas vinculadas:

a) A todos los entes que integran el sector público de Cataluña en los términos del artículo 2.1 de la Ley 29/2010, del 3 de agosto, del uso de los medios electrónicos en el sector público de Cataluña.
b) A cualquier otro ente que tenga que comunicarse o relacionarse por medios electrónicos con los entes del sector público de Cataluña según los términos definidos en el apartado anterior que promuevan el logro del modelo catalán de administración electrónica descrito en la Ley 29/2010 en el artículo 5 y que tiene como objetivos:
    i) La incorporación de los medios electrónicos en su actividad ordinaria para mejorar la accesibilidad, la transparencia, la eficacia, la eficiencia y la calidad de la prestación de servicios a los ciudadanos, y a la gestión interna.
    ii) La cooperación y la colaboración institucional en la creación y la puesta en disposición del sector público de Cataluña de infraestructuras y de servicios comunes de administración electrónica que garanticen la interoperabilidad de los sistemas de información y que hagan posible su uso por las entidades que integran el sector público para hacer más eficaz y económico el ofrecimiento de servicios a los ciudadanos y a las empresas.
    iii) La definición y el desarrollo común de políticas e iniciativas de carácter organizativo y tecnológico que maximicen la eficiencia y la reutilización de los servicios y las aplicaciones que los desarrollan.

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 Reglamento (UE) 910/2014.

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

- Certificado de autenticación de trabajador público de nivel alto (T-CAT autenticació).
- Certificado cualificado de firma de trabajador público de nivel alto (T-CAT signatura).
- Certificado cualificado de autenticación y firma de trabajador público de nivel medio (T-CATP).
- Certificado de autenticación de trabajador público con pseudónimo de nivel alto (T-CAT pseudònim autenticació).
- Certificado cualificado de firma de trabajador público con pseudónimo de nivel alto (T-CAT pseudònim signatura).
- Certificado cualificado de autenticación y firma de persona vinculada de nivel alto (T-CAT persona vinculada).
- Certificado cualificado de autenticación y firma de persona vinculada de nivel medio (T-CATP persona vinculada).

- Certificado cualificado de autenticación y firma de representante ante las Administraciones Públicas (T-CAT Representant).

Esta Política de Certificación está sujeta al cumplimiento de la Declaración de Prácticas de Certificación del Consorci AOC, la cual se hace referencia.

1.2. Nombre del documento e identificación

1.2.1. Identificación de este documento

Nombre:	PC Certificados Personales Sector Público
Versión:	6.0
Descripción	Política de Certificación para Certificados Personales del Sector Público
Fecha de emisión:	26/07/2018
OID:	1.3.6.1.4.1.15096.1.3.2.1.2
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 autenticación de trabajador público de nivel alto (T-CAT autenticació)	1.3.6.1.4.1.15096.1.3.2.7.1.2
Certificado cualificado de firma de trabajador público de nivel alto (T-CAT signatura)	1. 3.6.1.4.1.15096.1.3.2.7.1.1
Certificado cualificado de autenticación y firma de trabajador público de nivel medio (T-CATP)	1.3.6.1.4.1.15096.1.3.2.7.3.1
Certificado de autenticación de trabajador público con pseudónimo de nivel alto (T-CAT pseudònim autenticació)	1.6.1.4.1.15096.1.3.2.4.1.23
Certificado cualificado de firma de trabajador público con pseudónimo de nivel alto (T-CAT pseudònim signatura)	1.3.6.1.4.1.15096.1.3.2.4.1.1
Certificado cualificado de autenticación y firma de persona vinculada de nivel alto (T-CAT persona vinculada)	1.3.6.1.4.1.15096.1.3.2.82.1
Certificado cualificado de autenticación y firma de persona vinculada de nivel medio (T-CATP persona vinculada)	1.3.6.1.4.1.15096.1.3.2.86.1
Certificado cualificado de autenticación y firma de representante ante las Administraciones Públicas (T-CAT representant)	1.3.6.1.4.1.15096.1.3.2.8.1.1

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 su Autoridad de Certificación (en adelante CA, del inglés: Certification Authority) subordinada EC-SECTORPUBLIC.

2.2. Autoridades de Registro

Las Autoridades de Registro son las personas físicas o jurídicas que asisten al 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 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 firmantes o poseedores de claves.

- EL 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, que se identifican en el campo “Subject” del mismo.

2.3.3. Poseedores de claves o firmantes

Los poseedores de claves o firmantes son las personas físicas que poseen de forma exclusiva las claves de firma o autenticación digital de certificados, ya sea actuando en su propio nombre y derecho, o bien, mediante autorización del suscriptor, estando debidamente identificadas en el certificado mediante su nombre y apellidos o mediante un pseudónimo.

Corresponde al firmante o poseedor de claves la custodia de los datos de creación de firma o autenticación asociados al certificado digital.

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 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 hasta 5 años desde la fecha de su emisión, siempre que los mismos no resulten suspendidos o revocados.

3.2. Dispositivos de creación de firma

Lo siguientes certificados, emitidos al amparo de esta Política de Certificación, utilizan un dispositivo cualificado de creación de firma en cumplimiento de los requisitos establecidos en el Anexo II del Reglamento UE 910/2014:

- Certificados cualificado de autenticación y de firma de trabajador público de nivel alto (T-CAT autenticació y T-CAT signatura).
- Certificados cualificados de autenticación y de firma de trabajador público con pseudónimo de nivel alto (T-CAT pseudònim autenticació y T-CAT pseudònim signatura).
- Certificado cualificado de autenticación y firma de persona vinculada de nivel alto (T-CAT persona vinculada).
- Certificado cualificado de autenticación y firma de representante ante las Administraciones Públicas (T-CAT Representant).

El resto de certificados emitidos en el marco de esta Política de Certificación se emiten en software.

3.3. 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.

3.3.1. 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 autenticación de trabajador público de nivel alto (T-CAT autenticació)	● Autenticación personal y de atributos
Certificado cualificado de firma de trabajador público de nivel alto (T-CAT signatura)	● Firma electrónica

Certificado cualificado de autenticación y firma de trabajador público de nivel medio (T-CATP)	● Autenticación personal y de atributos ● Firma electrónica
Certificado de autenticación de trabajador público con pseudónimo de nivel alto (T-CAT pseudònim autenticació)	● Autenticación personal y de atributos
Certificado cualificado de firma de trabajador público con pseudónimo de nivel alto (T-CAT pseudònim signatura)	● Firma electrónica
Certificado cualificado de autenticación y firma de persona vinculada de nivel alto (T-CAT persona vinculada)	● Autenticación personal y de atributos ● Firma electrónica
Certificado cualificado de autenticación y firma de persona vinculada de nivel medio (T-CATP persona vinculada)	● Autenticación personal y de atributos ● Firma electrónica
Certificado cualificado de autenticación y firma de representante ante las Administraciones Públicas (T-CAT Representant)	● Autenticación personal y de atributos ● Firma electrónica

Los Certificados emitido 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 Usuaria que 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.

3.3.2. 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 prohibido 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 para la gestión de suspensiones de certificados.

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

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

En el caso de las Administraciones Públicas, la solicitud se enviará:

- A través de sus Autoridades de Registro T-CAT
- Directamente al Consorci AOC, de forma supletoria en caso de que el ente no tenga ninguna Autoridad de Registro asignada. En este caso el Consorci AOC actuará como Autoridad de Registro T-Cat

Esta solicitud requiere el envío de un documento con la información exacta y comprobada (certificada) de las personas, entidades o dispositivos para las cuales se pide el certificado. Esta tiene que ir firmada por la persona autorizada al efecto por la entidad suscriptora, y tiene que traer adjunto el certificado de esta información.

También se puede confirmar una dirección física u otros datos que permitan establecer contacto directo con el futuro poseedor de claves.

Toda la documentación se entrega a la Autoridad de Registro, por medios electrónicos. Podrá ser remitida en apoyo papel o mediante correo electrónico, excepcionalmente, por los siguientes motivos:

- Que la entidad suscriptora, por razón de su naturaleza jurídica, no pueda ser usuario del aplicativo informático usado para remitir las solicitudes (actualmente, EACAT)
- Que sea una entidad que solicite certificados digitales por primera vez, de forma que no disponga de ningún certificado digital con el que llevar a cabo la tramitación de la solicitud por medios electrónicos

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.

En este caso tiene que haber un documento, en soporte papel o electrónico, firmado por la Autoridad de Registro, que incluirá la indicación de la persona o personas a autorizar, por parte de la Autoridad de Certificación correspondiente, para realizar peticiones.

Los datos del usuario final necesarios para realizar la solicitud serán introducidos por el solicitante.

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, especialmente en caso de que sean intercambiados con el suscriptor, en caso de certificados individuales o con el tercer solicitante, en su caso.
- 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 RA validará la veracidad y exactitud de los datos del firmante comunicándoselo a la Autoridad de Certificación.

El operador de RA 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 o autenticación y, por otro lado, al cabo de 3 días, el acceso al propio dispositivo.

4.3.5. Emisión del certificado

El Operador de RA 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 RA autorizado. Tras esta validación se procederá a la emisión del certificado.

4.3.6. 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 del siguiente material:
    - Hoja de entrega de poseedor
    - Dispositivo criptográfico o en software 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 del dispositivo y también en el tiempo.

4.3.7. Suspensión de certificados

Según se detalla en la DPC.

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 autenticación de trabajador público de nivel alto (T-CAT autenticació)	1.3.6.1.4.1.15096.1.3.2.7.1.2
Certificado cualificado de firma de trabajador público de nivel alto (T-CAT signatura)	1.3.6.1.4.1.15096.1.3.2.7.1.1
Certificado cualificado de autenticación y firma de trabajador público de nivel medio (T-CATP)	1.3.6.1.4.1.15096.1.3.2.7.3.1
Certificado de autenticación de trabajador público con pseudónimo de nivel alto (T-CAT pseudònim autenticació)	1.3.6.1.4.1.15096.1.3.2.4.1.2
Certificado cualificado de firma de trabajador público con pseudónimo de nivel alto (T-CAT pseudònim signatura)	1.3.6.1.4.1.15096.1.3.2.4.1.1
Certificado cualificado de autenticación y firma de persona vinculada de nivel alto (T-CAT persona vinculada)	1.3.6.1.4.1.15096.1.3.2.82.1
Certificado cualificado de autenticación y firma de persona vinculada de nivel medio (T-CATP persona vinculada)	1.3.6.1.4.1.15096.1.3.2.86.1
Certificado cualificado de autenticación y firma de representante ante las Administraciones Públicas (T-CAT Representant)	1.3.6.1.4.1.15096.1.3.2.8.1.1

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