Consorci
Administració Oberta
de Catalunya

Declaración de Prácticas de Certificación
Entidad de CertificaciónGENCAT
(EC-GENCAT)

Referencia:	D1111_E0650_N-DPC EC-GENCAT
Versión:	2.0
Fecha:	05/08/2016

Control documental

Estado formal	**Elaborado por:** Servei de Certificació Digital	**Aprobado por:** Direcció del Consorci AOC
Fecha de creación	02/10/2014	
Control de versiones	**Fecha:**	05/08/2016
	Descripción:	Revisión Global – Integración CATCert en Consorci AOC
Nivel de acceso información	pública	
Título	Declaración de Prácticas de Certificación – Entidad de CertificaciónGENCAT	
Fichero	D111 E0650 N-DPC EC-GENCAT v2r0 CAS	
Control de copias	Sólo las copias disponibles en https://www.aoc.cat/ garantizan la actualización de los documentos. Toda copia impresa o guardada en ubicaciones diferentes se considerarán copias no controladas.	
Derechos de Autor		

Índice

1. Introducción

Este documento es la Declaración de Prácticas de Certificación de la Entidad de Certificación 'GENCAT (en adelante EC-GENCAT, Entidad de Certificación Raíz de la jerarquía pública de certificación de Catalunya.

En esta DPC se regulan técnicamente y operativamente los servicios de certificación de la EC-GENCAT.

Los apartados con el contenido "Sin estipulación adicional" indican que se debe consultar la Política General de Certificación del Consorcio AOC.

1.1 Presentación

En desarrollo del pacto institucional firmado el 23 de julio del 2001 por los grupos parlamentarios del Parlament de Catalunya, la Generalitat de Catalunya y el Consorci d'Ens Locals de Catalunya (Localret), para el desarrollo de políticas que permitan afrontar el cambio fundamental en las estructuras sociales y económicas derivado de la confluencia de las nuevas tecnologías de la información y la comunicación en el ámbito de las administraciones públicas catalanas, se decidió establecer sistemas de interrelación entre dichas administraciones, y entre las administraciones y los ciudadanos, por vía telemática y electrónica, en las condiciones de seguridad necesarias y, especialmente, haciendo uso de certificados digitales de identidad y firma electrónica.

En cumplimiento de dicho pacto institucional y para desarrollar el programa Catalunya en Xarxa (Cataluña en Red), Localret y la Generalitat de Catalunya acordaron la creación del Consorci per a l'Administració Oberta Electrònica de Catalunya (Consorcio para la Administración Abierta Electrónica de Catalunya), con la finalidad de desarrollar políticas públicas en materia de servicios electrónicos a las administraciones públicas y de ejercer la condición de autoridad (técnica) de certificación de firma electrónica para garantizar el secreto, la integridad, la identidad y la autenticidad en las comunicaciones y documentos electrónicos que se producen en el ámbito de las administraciones públicas catalanas.

El 25 de febrero de 2002 tuvo lugar la sesión constitutiva del Consorci per a l'Administració Oberta Electrònica de Catalunya, una sesión en que el Consejo General adoptó, entre otros, el acuerdo de constituir un ente de gestión directa bajo la forma de organismo autónomo de carácter comercial, con la denominación de Agència Catalana de Certificació (CATCert), con el objeto de gestionar certificados digitales y prestar otros servicios relacionados con la firma electrónica en el ámbito público catalán.

CATCert se creó por acuerdo de la Comisión Ejecutiva del Consorci de l'Administració Oberta Electrónica de Catalunya, de 29 de abril de 2002, como organismo autónomo de carácter comercial, los estatutos de la cual fueron publicados en el Diario Oficial de la Generalitat de Catalunya el 30 de mayo de 2003, por Resolución PRE/1574/2003, de 15 de mayo.

Por tanto, la Agencia Catalana de Certificació se constituyó en la entidad principal del sistema público catalán de certificación que regulaba la emisión y la gestión de los certificados que se emitieranpara las instituciones de autogobierno de Catalunya, las instituciones que integran el mundo local, y el resto de entidades públicas y privadas que integran el sector público catalán; así como la admisión y el uso de los certificados emitidos a ciudadanos y empresas por otros prestadores de servicios de certificación y que solicitaran la correspondiente clasificación.

Estas instituciones emitirán certificados por medio de una infraestructura técnica proporcionada por CATCert, denominada “jerarquía pública de certificación de Catalunya”, y podrán admitir y utilizar certificados de otros prestadores mediante los servicios de clasificación y validación de CATCert.

En este sentido, CATCert creó el 8 de agosto de 2003 una jerarquía de entidades de certificación, la raíz de la cual es la propia Agencia.

La Entidad de certificación GENCAT (denominada EC-GENCAT) se creó para satisfacer las necesidades de la Administración de la Generalitat de Catalunya. Posteriormente, se creó la Entidad de Certificación de Secretaria de Administraciói Funció Pública, bajo la jerarquía de la EC-GENCAT. La EC-SAFP es la entidad de certificación que emite certificados al usuario final, de modo que la EC-GENCAT se mantiene operativa para garantizar el funcionamiento de la jerarquía, pero no emite certificados a usuarios finales, emitiendo solamente los certificados de infraestructura correspondientes.

Actualmente existen nueve entidades de certificación vinculadas a la jerarquía pública de certificación de las administraciones públicas catalanas: EC-GENCAT, EC-SAFP, EC-AL, EC-IdCAT, EC-UR, EC-URV, EC-Parlament, EC-SectorPublic y EC-Ciutadania.

El Acuerdo de Gobierno de 16 de octubre de 2013 asigna la prestación de servicios de certificación al Consorci Administració Oberta de Catalunya (AOC), como medida de racionalización del sector público, que se concreta en la integración de la Agència Catalana de Certificació en el Consorci AOC, en el cual revertirán todas las marcas, derechos, deberes y servicios gestionados hasta la fecha por CATCert.

La integración se hizo efectiva meidante el citado acuerdo con efectos contables y jurídicos el 30 de junio de 2013, fecha en la cual el Consorci AOC asume los derechos y obligaciones, así como la prestación del servicio, incluyendo el Servicio de Certificación Digital, responsable de la emisión y gestión del ciclo de vida de los certificados digitales. En adelante, el Consorci Administració Oberta de Catalunya es el prestador de los servicios de certificación (TSP) públicos de Catalunya y el propietario de la infraestructura de clave pública (PKI) que antes era titularidad de CATCert.

1.1.1 Tipos y clases de certificados

La EC-GENCAThа definido una tipología de servicios de certificación que le permitenemitir certificados digitales para diversos usos y usuarios finales diferentes.

Los certificados de infraestructura son aquellos que se emiten para gestionar y operar la infraestructura de clave pública (PKI), que es el sistema técnico, jurídico, de seguridad y de organización que da soporte a los servicios de certificación y de firma electrónica.

LaEC-GENCAT emite los siguientes tipos de Certificados de infraestructura:

1) Certificado de infraestructura de entidad de certificación vinculada (CIC), que se expide a las Entidades de Certificación que se vinculan a la jerarquía.

   Las Entidades de Certificación vinculadas pueden, a su vez, emitir certificados de infraestructura o certificados de entidad final (personales, de entidad y de dispositivo), según la clase del certificado CIC que posean, desde el momento en el que hayan obtenido un certificado CIC válido, y mientras dicho certificado se encuentre vigente.

2) Certificado de infraestructura personal de firma electrónica reconocida de operadores (CIPISR), que se utiliza para autorizar operaciones relacionadas con los servicios de certificación, como la aprobación de solicitudes de certificación.

3) Certificado de infraestructura de dispositivo servidor seguro (CIDS), que es utilizado para una aplicación informática servidor de SSL o de TLS de infraestructura para identificarse ante las aplicaciones cliente que se conecten y para proteger el secreto de las comunicaciones entre el cliente y el servidor, como por ejemplo los servidores de las entidades de certificación.

4) Certificado de infraestructura de dispositivo de aplicación digitalmente asegurada (CIDA), que es utilizado para aplicaciones informáticas de la infraestructura que se identifiquen digitalmente, firmen electrónicamente webservices u otros protocolos y que reciban documentos y mensajes cifrados, como por ejemplo las aplicaciones de notificación de mensajes de las entidades de certificación.

5) Certificado de infraestructura de servidor de estado de certificados en línea (CIO), que es utilizado por un servidor OCSP Responder para firmar sus respuestas sobre el estado de validez de los certificados.

6) Certificado de infraestructura de entidad de sellos de tiempo (CIT), que es utilizado por una entidad para firmar los sellos de tiempo que emite.

7) Certificado de infraestructura de entidad de validación (CIV), que es utilizado por un servidor de entidad de validación para firmar sus informes.

1.1.1.1 Certificado de infraestructura de entidad de certificación vinculada (CIC)

Los Certificados CIC son aquellos certificados de infraestructura emitidos, únicamente a otras Entidades de Certificación, que, de esta forma, quedan vinculadas a la jerarquía pública de certificación de Cataluña.

Los certificados CIC se expiden para ofrecer servicios a una comunidad de usuarios concreta dentro de la jerarquía pública de certificación de Cataluña, pudiendo ser de diferentes niveles (nivel 1, 2 o sucesivos).

Con estos Certificados, se faculta a las Entidades de Certificación a emitir certificados a usuarios finales o a otras Entidades de Certificación dentro de su propia comunidad de usuarios, en función de sus necesidades concretas, y siempre que técnicamente no afecte al funcionamiento, plataformas, sistemas y aplicaciones habitualmente empleados por los usuarios finales.

Cada certificado CIC recibe un nivel, adecuado al período de duración del mismo, que se utilizará para la programación de la renovación periódica de la infraestructura de certificación.

Estos certificados permiten que las Entidades de Certificación suscriptoras puedan expedir certificados a otros usuarios, ya sean otras Entidades de Certificación de nivel inferior dentro de la jerarquía, ya sean entidades finales (personales, de entidad, de dispositivo y de objeto), desde el momento en que hayan obtenido un certificado CIC válido y mientras éste se halle vigente.

Estos certificados son, generalmente, emitidos por el Consorci AOC, como Entidad de Certificación Raíz, a organizaciones que operan una Entidad de Certificación dentro de su jerarquía, para diferentes usos, según su clase.

Estos Certificados CIC se obtienen después de un proceso de admisión de la EC Vinculada a los servicios de certificación del Consorci AOC, proceso descrito en la Política General de Certificación del Consorci AOC.

La futura EC Vinculada no podrá solicitar el Certificado CIC hasta que haya completado su procedimiento de admisión, en la Jerarquía de Entidades de Certificación de Catalunya, de acuerdo con la Política General de Certificación del Consorci AOC.

1.1.1.2 Certificado de infraestructura personal de firma electrónica reconocida de operadores (CIPISR)

Los CIPISR son certificados de infraestructura emitidos a operadores de Entidades de Registro, para los trabajos de emisión y gestión del ciclo de vida de certificados de una Entidad de Certificación.

Por consiguiente, estos certificados únicamente se utilizan para autorizar operaciones relacionadas con los servicios de certificación, como la aprobación de solicitudes de certificación, no pudiendo ser utilizados para ningún otro uso que no sea el de operador de Entidad de Registro.

Los CIPISR se emiten en dos modalidades: de clase 1 y de clase 2. Los CIPISR de clase 1 se expiden a operadores de Entidades de Registro en el ámbito de las instituciones integrantes del sector público catalán; mientras que los CIPISR de clase 2 se expiden a operadores de entornos cerrados de usuarios en el ámbito privado.

La duración de la licencia de los CIPISR, de clase 1 y 2, es de cuatro (4) años, a contar desde la fecha de su emisión.

1.1.1.3 Certificado de infraestructura de dispositivo servidor seguro (CIDS)

Los CIDS son certificados de infraestructura emitidos a Entidades de Certificación responsables de la operación de servidores seguros SSL o TLS con la finalidad de identificarse ante las aplicaciones cliente que se conecten y la protección del secreto de las comunicaciones entre el cliente y el servidor.

Los certificados CIDS se caracterizan por el hecho de 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 del suscriptor del certificado.

Los certificados CIDS son certificados destinados a ser utilizados exclusivamente en un servidor del suscriptor identificado en el propio certificado, que le identifican electrónicamente y protegen la información entre el cliente y el servidor. Por ello, es condición esencial para la validez del certificado CIDS la especificación de los sistemas del suscriptor en los que serán utilizados los certificados.

La duración de la licencia de los CIDS es de cuatro (4) años, a contar desde la fecha de su emisión.

1.1.1.4 Certificado de infraestructura de dispositivo de aplicación digitalmente asegurada (CIDA)

Los certificados CIDA son certificados de infraestructura, emitidos a Entidades de Certificación responsables de la operación de aplicaciones informáticas que se identifican

digitalmente, firman electrónicamente webservices u otros protocolos y reciben documentos y mensajes cifrados.

Como certificado de dispositivo, los certificados CIDA se caracterizan por el hecho de 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 del suscriptor del certificado.

Los certificados CIDA son certificados destinados a ser utilizados exclusivamente en un dispositivo del suscriptor identificado en el propio certificado, y por ende, en los sistemas del suscriptor del certificado.

La duración de la licencia de los CIDA es de cuatro (4) años, a contar desde la fecha de su emisión.

1.1.1.5 Certificado de infraestructura de servidor de estado de certificados en línea (CIO)

Los certificados CIO son aquellos certificados de infraestructura, emitidos para gestionar los servicios de certificación, que se expiden a Entidades responsables de la operación de servidores OCSP Responder, para firmar sus respuestas sobre el estado de validez de los certificados.

Los certificados CIO son certificados destinados a ser utilizados exclusivamente en un servidor OCSP Responder de la Entidad suscriptora, servidor que se encuentra identificado en el propio certificado. Por ello, es condición esencial para la validez del certificado CIO la especificación de los sistemas del suscriptor en los que serán utilizados los certificados.

La duración de la licencia de los CIO es de cuatro (4) años, a contar desde la fecha de su emisión.

1.1.1.6 Certificado de infraestructura de entidad de sellos de tiempo (CIT)

Los certificados CIT son certificados expedidos a las Entidades responsables de la operación de autoridades de sellado de tiempo y hora (en lo sucesivo, TSA), que se utilizan para firmar los sellos de tiempo que éstas emiten.

Los CIT son certificados ordinarios, que sirven para gestionar los servicios de certificación y para garantizar la fecha y la hora de un determinado acto.

La duración de la licencia de los CIT es de cuatro (4) años, a contar desde la fecha de su emisión.

Los certificados CIT son emitidos exclusivamente para que las Entidades suscriptoras firmen los sellos de tiempo que emiten.

1.1.1.7 Certificado de infraestructura de entidad de validación (CIV)

Los certificados CIV son certificados de infraestructura, emitidos para gestionar los servicios de certificación, que se expiden a Entidades de Validación para que firmen los informes de validación que emiten.

El certificado CIV ofrece, respecto de los Informes de Validación firmados con éste, las garantías siguientes:

- Garantía de verificación de los certificados o firmas respecto de los cuales se haya realizado la solicitud del Informe de Validación.

- Garantía del contenido de los referidos certificados o firmas previamente verificados.
- Garantía de la fecha y hora del informe.

La duración de la licencia de los CIV es de cuatro (4) años, a contar desde la fecha de su emisión.

Adicionalmente, en función de requerimientos técnicos y las necesidades de los usuarios, es posible que los citados tipos de certificados puedan incorporar otras funcionalidades que, en todo caso, serán identificados en cada política específica de certificación, que deberá ser aprobada por el Consorci AOC.

1.1.2 Relación entre la Declaración de Prácticas de Certificación (DPC) y otros documentos

Este documento contiene la declaración de prácticas de certificación de la EC-GENCAT.

La EC-GENCATemite certificados dentro de la jerarquía de certificación operada por el Consorci AOC, por tanto tiene que disponer de una declaración de prácticas de certificación, de acuerdo con la política general de certificación del Consorci AOC.

Esta DPC incluye los procedimientos que aplica la EC-GENCAT en la prestación de sus servicios, en cumplimiento de los requisitos establecidos por las políticas que gestiona y el artículo 19 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

Esta DPC se relaciona con la documentación auxiliar, entre la cual se encuentran los instrumentos jurídicos reguladores de la prestación del servicio, de la documentación y de las políticas de seguridad, así como de la documentación de operaciones.

1.2 Nombre del documento e identificación

1.2.1 Identificación de este documento

Este documento se denomina “Declaración de Prácticas de Certificación (DPC) de la EC-GENCAT”.

Esta Declaración de Prácticas de Certificación se identifica con el siguiente OID:

1.3.6.1.4.1.15096.1.2.3

1.2.2 Identificación de políticas de certificación cubiertas por esta DPC

La EC-GENCAT emite y gestiona certificados de acuerdo con las siguientes políticas:

- **CIC.-Certificado de infraestructura de entidad de certificación vinculada**

  - Los CIC de nivel 2se identifican con el identificador de objeto (OID): 1.3.6.1.4.1.15096.1.3.1.12.

- **Certificado de Infraestructura de la Entidad de Certificación de la Secretaria d'Administració i Funció Pública (EC-SAFP)**

El certificado CIC de la EC-SAFP es de nivel 2 y se identifica con el identificador de objeto (OID): 1.3.6.1.4.1.15096.1.3.1.12.

- **CIPISR.- Certificado de infraestructura personal de firma electrónica reconocida de operadores**

  Los certificados CIPISR de clase 1 emitidos por la EC-GENCATse identifican con el identificador de objeto (OID): 1.3.6.1.4.1.15096.1.3.1.15.

  Los certificados CIPISR de clase 2 emitidos por la EC-GENCAT se identifican con el identificador de objeto (OID): 1.3.6.1.4.1.15096.1.3.1.16.

- **Certificado de infraestructura de dispositivo servidor seguro (CIDS)**

  Los certificados CIDS de clase 1 emitidos por la EC-GENCATse identifican con el identificador de objeto (OID): 1.3.6.1.4.1.15096.1.3.1.17.

- **Certificado de infraestructura de dispositivo de aplicación digitalmente asegurada (CIDA)**

  Los certificados CIDA de clase 1 emitidos por la EC-GENCATse identifican con el identificador de objeto (OID): 1.3.6.1.4.1.15096.1.3.1.18.

- **Certificado de infraestructura de servidor de estado de certificados en línea (CIO)**

  Los certificadosCIO de clase 1emitidos por la EC-GENCATse identifican con el identificador de objeto (OID): 1.3.6.1.4.1.15096.1.3.1.19.

- **Certificado de infraestructura de entidad de sellos de tiempo (CIT), que es utilizado por una entidad para firmar los sellos de tiempo que emite**

  Los certificadosCIT de clase 1emitidos por la EC-GENCATse identifican con el identificador de objeto (OID): 1.3.6.1.4.1.15096.1.3.1.111.

- **Certificado de infraestructura de entidad de validación (CIV)**

  Los certificadosCIV de clase 1emitidos por la EC-GENCATse identifican con el identificador de objeto (OID): 1.3.6.1.4.1.15096.1.3.1.20.

Els documents descriptius d'aquests perfils de certificats es publiquen en el web del Consorci AOC

1.3 Comunidad de usuarios de certificados

La presente DPC regula una comunidad de usuarios, que obtienen certificados para diversas relaciones administrativas y privadas, de acuerdo con la Ley 59/2003, de 19 de diciembre, de firma electrónica y la normativa administrativa correspondiente.

Los certificados de infraestructura de la EC-GENCAT no se expiden al público, sino a:

- La Entidad de Certificación de la Secretaria d'Administració i Funció Pública (EC-SAFP).

1.3.1 Prestadores de servicios de certificación

Un prestador de servicios de certificación es una persona física o jurídica que produce certificados y presta otros servicios en relación con la firma electrónica, de acuerdo con la Ley 59/2003, de 19 de diciembre, de firma electrónica.

El prestador de servicios de certificación genera los certificados digitales mediante la operación de entidades de certificación de su titularidad que firman los certificados.

El Consorci AOC será el prestador de servicios de certificación de la EC-GENCAT.

En su función de prestador de servicios de certificación,el Consorci AOC será responsable dela actuación de la EC-GENCAT ante los usuarios finales y los terceros verificadores de certificados y firmas electrónicas, por la actuación de las autoridades de certificación que operan en nombre de las diferentes entidades de certificación.

1.3.2 Entidad de Certificación Raíz

El Consorci AOC dispone de una autoridad de certificación principal, que es la raíz de la jerarquía pública de certificación de Cataluña: la EC-GENCAT, cuya finalidad es integrar otras entidades de certificación en el sistema público catalán de certificación mediante la vinculación técnica de las autoridades de certificación correspondientes.
La citada vinculación técnica se consigue mediante la emisión de certificados de infraestructura de entidad de certificación vinculada (CIC).

1.3.3 EC-GENCAT

La EC-GENCAT es la Entidad de Certificación del sector público de Catalunya, vinculada a la jerarquía de entidades de certificación de las entidades públicas de Catalunya, que emite los certificados indicados en el punto 1.1.1.

La huella digital del certificado de la EC-GENCAT es:

```
f0 b7 5b b7 93 11 b0 e5 d0 10 f1 ed 8d c7 e5 8f 15 be 68 fd
```

1.3.4 Entidades de Registro

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

1.3.5 Usuarios finales

Los usuarios finales son las personas (físicas o jurídicas) que obtienen y utilizan los certificados personales, de entidad y de dispositivo emitidos por la EC-GENCAT;concretamente, podemos distinguir los siguientes usuarios finales:

- Los solicitantes de certificados
- Los suscriptores de certificados o los titulares de certificados
- Los poseedores de claves.
- Los verificadores de firmas y de los certificados

1.3.5.1 Solicitantes de certificados

Los solicitantes de los certificados indicados en la presente DPC son las personas autorizadas por las Entidades de Certificación suscriptora.

Pueden ser solicitantes:

- La persona que será el futuro poseedor de claves.
- Una persona autorizada por:
    - La Entidad de Certificación Raíz de la jerarquía (EC-ACC).
    - La Entidad de Certificación de la Generalitat de Catalunya (EC-GENCAT).
    - La Entidad de Certificación SectorPúblic (EC-SECTORPUBLIC)
    - La Entidad de Certificación Ciutadania (EC-CIUTADANIA)
    - La Entidad de Certificación de la Secretaria d'Administració i Funció Pública (EC-SAFP).
    - La Entidad de Certificación de Ciudadanos (EC-idCAT).
    - La Entidad de Certificación de la Administració Local (EC-AL).
    - La Entidad de Certificación d'Universitats i Recerca (EC-UR).
    - La Entidad de Certificación del Parlament de Catalunya (EC-Parlament).

La autorización podrá realizarse de forma expresa o tácita y, en aquellos casos en los que la EC-GENCAT lo considere conveniente, deberá formalizarse documentalmente.

1.3.5.2 Suscriptores de certificados

Los suscriptores de los certificados son instituciones y las personas, físicas o jurídicas, identificados en el campo "Subject" del certificado.

El suscriptor de los certificados de infraestructura es:

- La Entidad de Certificación SectorPúblic (EC-SECTORPÚBLIC)
- La Entidad de Certificación Ciutadania (EC-CIUTADANIA)
- La Entidad de Certificación de la Secretaria d'Administració i Funció Pública (EC-SAFP).
- La Entidad de Certificación de Ciudadanos (EC-idCAT).

- La Entidad de Certificación de la Administració Local (EC-AL).
- La Entidad de Certificación de la Universitat i Recerca (EC-UR).
- La Entidad de Certificación del Parlament de Catalunya (EC-Parlament).

1.3.5.3 Poseedores de claves

Los poseedores de claves son las personas físicas que poseen de forma exclusiva las claves de firma digital de certificados personales o de entidad, de clase 1 o 2 de organización, que se encuentran debidamente autorizadas para ello por el suscriptor y debidamente identificados en el certificado mediante su nombre y apellidos o mediante un seudónimo (posibilidad esta última únicamente aplicable a los certificados de clase 2).

1.3.5.4 Usuarios de certificados

Los usuarios de los certificados son los verificadores.

1.3.5.5 Verificadores de certificados

Los verificadores son las personas (incluyendo personas físicas, instituciones, personas jurídicas y otras organizaciones y entidades) que reciben firmas digitales y certificados digitales y tienen que verificarlos, como paso previo a confiar en las mismas.

1.4 Uso de los certificados

Esta sección lista las aplicaciones para las que puede utilizarse cada tipo de certificado, estableciendo limitaciones y prohíbe algunas aplicaciones de los certificados.

1.4.1 Usos típicos de los certificados

1.4.1.1 Certificado de infraestructura de entidad de certificación vinculada que se emite a las Entidades de Certificación que se vinculan a la jerarquía

Estos certificados permiten que las Entidades de Certificación suscriptoras puedan expedir certificados a otros usuarios, ya sean otras Entidades de Certificación de nivel inferior dentro de la jerarquía, ya sean entidades finales (personales, de entidad, de dispositivo y de objeto), desde el momento en que hayan obtenido un certificado CIC válido y mientras éste se halle vigente.

Estos certificados son, generalmente, emitidos por la Agència Catalana de Certificació, como EC Raíz, a organizaciones que operan una EC dentro de su jerarquía, para diferentes usos, según su clase:

- Firma de peticiones de renovación, suspensión y revocación de certificados CIC.
- Emisión y firma de certificados CIC, CIPISR, CIDS, CIDA, CIO, CIT iCIV.
- Emisión y firma de listas de revocación de certificados (LRC).

a. Certificado de Infraestructura de Entidad de Certificación

Los usos permitidos del certificado CIC de la EC-ACC son:

- Firma de peticiones de renovación, suspensión y revocación de certificados CIC.
- Emisión y firma de certificados CIC, CIPISR, CIDS, CIDA, CIO, CIT y CIV.
- Emisión y firma de listas de revocación de certificados (LRC).

1.4.1.2 Certificado de infraestructura personal de firma electrónica reconocida de operadores (CIPISR)

Estos Certificados permiten que los operadores de Entidades de Registro realizar los trabajos de emisión y gestión del ciclo de vida de certificados de una Entidad de Certificación.

Por consiguiente, estos certificados únicamente se utilizan para autorizar operaciones relacionadas con los servicios de certificación, como la aprobación de solicitudes de certificación, no pudiendo ser utilizados para ningún otro uso que no sea el de operador de Entidad de Registro.

1.4.1.3 Certificado de infraestructura de dispositivo servidor seguro (CIDS)

Estos Certificados permiten que las Entidades de Certificación responsables de la operación de servidores seguros SSL o TLS:

- Se identifiquen ante las aplicaciones cliente que se conecten, y
- Protejan el secreto de las comunicaciones entre el cliente y el servidor.

Los Certificados CIDS están destinados a ser utilizados exclusivamente en un servidor del suscriptor identificado en el propio certificado, que le identifican electrónicamente y protegen la información entre el cliente y el servidor. Por ello, es condición esencial para la validez del certificado CIDS la especificación de los sistemas del suscriptor en los que serán utilizados los certificados.

1.4.1.4 Certificado de infraestructura de dispositivo de aplicación digitalmente asegurada (CIDA)

Estos Certificados permiten que las Entidades de Certificación responsables de la operación de aplicaciones informáticas que se identifican digitalmente, firmen electrónicamente webservices u otros protocolos y reciben documentos y mensajes cifrados.

Los Certificados CIDA están destinados a ser utilizados exclusivamente en un dispositivo del suscriptor identificado en el propio certificado, y por ende, en los sistemas del suscriptor del certificado.

1.4.1.5 Certificado de infraestructura de servidor de estado de certificados en línea (CIO)

Estos Certificados permiten que las Entidades responsables de la operación de servidores OCSP Responder firmen sus respuestas sobre el estado de validez de los certificados.

Los certificados CIO son certificados destinados a ser utilizados exclusivamente en un servidor OCSP Responder de la Entidad suscriptora, servidor que se encuentra identificado en el propio certificado. Por ello, es condición esencial para la validez del certificado CIO la especificación de los sistemas del suscriptor en los que serán utilizados los certificados.

1.4.1.6 Certificado de infraestructura de entidad de sellos de tiempo (CIT)

Estos Certificados permiten que las Entidades responsables de la operación de autoridades de sellado de tiempo y hora (en lo sucesivo, TSA), firmen los sellos de tiempo que éstas emiten.

Los CIT son certificados ordinarios, que sirven para gestionar los servicios de certificación y para garantizar la fecha y la hora de un determinado acto.

1.4.1.7 Certificado de infraestructura de entidad de validación (CIV)

Estos Certificados permiten que las Entidades de Certificación, actuando como Entidades de Validación, firmen los informes de validación que emiten.

1.4.2 Aplicaciones prohibidas

1.4.2.1 Informaciones para todos los tipos de certificados

Los certificados sólo podrán ser utilizados dentro de los límites de uso recogidos de manera expresa en su licencia de uso y sus correspondientes Condiciones de Uso. Cualesquiera otros usos fuera de los descritos en los citados documentos, quedan expresamente excluidos del ámbito contractual y formalmente prohibidos.

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 requieran 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 pudiera directamente comportar la muerte, lesiones personales o daños medioambientales severos.

1.4.2.2 Requisitos específicos para los CIC

Los certificados CIC se atendrán a lo dispuesto en esta DPC y, en todo caso, las limitaciones estarán delimitadas por la clase de certificado CIC y por la política del certificado en cuestión.

1.4.2.3 Requisitos específicos para los CIPISR

Los CIPISR no pueden utilizarse para ningún otro uso que el de operador de Entidad de Registro.

1.4.2.4 Requisitos específicos para los CIDS, CIDA, CIO, CIT y CIV

Los CIDS, CIDA, CIO, CIT y CIV no pueden utilizarse en sistemas diferentes de los de Entidad de Certificación.

1.5 Administración de la Declaración de Prácticas.

1.5.1 Organización que administra la especificación

Consorci Administració Oberta de Catalunya – Consorci AOC

1.5.2 Datos de contacto de la organización

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: www.aoc.cat

Web del servicio de certificación digitaldel Consorci AOC:

www.aoc.cat/catcert

Servicio de Atención al Usuario: 902 901 080, en horario 24x7 para la gestión de suspensiones de certificados.

1.5.3 Persona que determina la conformidad de una Declaración de Prácticas de Certificación (DPC) con la política

La persona que determina la conformidad de una DPC con la Política General de Certificación es el/la Responsable del Servicio de Certificación Digital del Consorci AOC, basándose en los resultados de una auditoría al efecto, realizada por un tercero, bianualmente.

1.5.4 Procedimiento de aprobación

El sistema documental y de organización de la EC-GENCAT garantiza, mediante la existencia y la aplicación de los correspondientes procedimientos, el correcto mantenimiento de la Declaración de prácticas de certificación y de las especificaciones de servicio relacionadas con ella.

Esto incluye el procedimiento de modificación de especificación del servicio y el procedimiento de publicación de especificaciones de servicio.

LA versión inicial de esta Declaración de prácticas es aprobada por la Comisión Ejecutiva del Consorci AOC, que es el órgano colegiado de dirección ejecutiva del Consorci AOC.

El Director Gerente del Consorci AOC es competente para aprobar las sucesivas modificaciones de esta Declaración de prácticas.

2. Publicación de información y directorio de certificados

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 fallo del sistema fuera de control de la EC-GENCAT, ésta realiza sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo en el plazo establecido en la sección 5.7.4 de la presente DPC.

2.2. Publicación de información de la EC-GENCAT

La EC-GENCAT publica las siguientes informaciones, en su web (http://www.aoc.cat/catcert/):

a) Las listas de certificados revocados y otras informaciones de estado de revocación de los certificados.

b) La política general de certificación y, cuando sea conveniente, las políticas específicas.

c) Los perfiles de los certificados y de las listas de revocación de los certificados.

d) La Declaración de Prácticas de Certificación.

e) Los instrumentos jurídicos vinculantes con suscriptores y verificadores.

Todo cambio en las especificaciones o condiciones del servicio se comunica a los usuarios por la EC-GENCAT, a través del Directorio.

En todos los casos se hace una referencia explícita a los cambios en la página principal del Web del servicio.

No se retira la versión anterior del documento objeto del cambio, pero se indica que ha sido sustituido por la versión nueva.

2.3. Frecuencia de publicación

La información de la EC-GENCAT se publica cuando se encuentra disponible y en especial, de forma inmediata cuando se emiten las menciones relativas a la vigencia de los certificados.

Los cambios en este documento se rigen por lo establecido en la sección **Error! No s'ha trobat l'origen de la referència.***Procedimiento para las modificaciones.*

Al cabo de 15 (quince) días desde la publicación de la nueva versión, se retira la referencia al cambio de la página principal y se inserta en el directorio.

Las versiones antiguas de la documentación son conservadas, por un periodo de 15 (quince) años por la EC-GENCAT, pudiendo ser consultadas por los interesados.

La información de estado de revocación de certificados se publica de acuerdo con lo establecido en la sección 4.10.7.

2.4. Control de acceso

Sin estipulación adicional.

3. Identificación y autenticación

3.1. Gestión de nombres

En esta sección se establecen requisitos relativos a los procedimientos de identificación y autenticación que se utilizan durante las operaciones de registro que realizan, con anterioridad a la emisión y entrega de certificados, las Entidades de Registro.

3.1.1. Tipos de nombres

3.1.1.1 Estructura sintáctica

Todos los certificados contienen unnombre diferenciado X.501 en el campo Subject, incluyendo un componente Common Nave (CN=).

La estructura sintàctica y el contenido de los campos de cada certificado, así como su significado semántico se encuentran descritos en el documento “perfil de certificado” correspondiente que el Consorci AOC publica en su web (http://www.aoc.cat/catcert/).

3.1.1.2 Perfils dels certificats

Els perfils dels certificats emesos per l’EC-GENCAT es publiquen al web del Consorci AOC (http://www.aoc.cat/catcert/).

3.1.2. Significado de los nombres

Sin estipulación adicional.

3.1.3. Utilización de anónimos y pseudónimos

No se pueden usar pseudónimos para identificar a una organización.

3.1.4. Interpretación de formatos de nombres

Sin estipulación adicional.

3.1.5. Unicidad de los nombres

La EC-GENCAT emite diferentes tipos de certificados. Los nombres de los suscriptores de certificados son únicos, para cada servicio de generación de certificados operado por la EC-GENCAT y para cada tipo de certificado; es decir, una misma persona sólo puede tener a su nombre, certificados de tipos diferentes emitidos por la EC-GENCAT.

No se puede volver a asignar un nombre de suscriptor que ya haya sido ocupado a un suscriptor diferente.

3.1.6. Resolución de conflictos relativos a nombres

Sin estipulación adicional.

Referente al tratamiento de marcas registradas, ver el apartado **Error! No s'ha trobat l'origen de la referència.**.

3.2. Validación inicial de la identidad

3.2.1. Prueba de posesión de clave privada

Sin estipulación adicional.

3.2.2. Autenticación de la identidad de una organización

Esta sección contiene los requisitos para la comprobación de la identidad de una organización identificada en el certificado.

En general, la EC-GENCAT no tendrá que determinar que un solicitante de certificados tiene derecho sobre el nombre que aparece en una solicitud de certificado. Tampoco actuará como árbitro o mediador, ni de ninguna otra manera tendrá que resolver ninguna disputa concerniente a la propiedad de nombres de personas u organizaciones, nombres de dominio, marcas o nombres comerciales (por ejemplo, relativos a direcciones electrónicas).

3.2.2.1. Entidades de Certificación Vinculadas

No se requiere realizar procedimiento de autenticación de las Entidades de Certificación Vinculadas a la jerarquía pública de certificación del Consorci AOC , por cuanto éstas se crean en el seno de la jerarquía mediante un procedimiento aprobado por la propia EC-GENCAT denominado “Ceremonia de Claves”, descrito en la sección correspondiente de la presente DPC.

3.2.2.2 Entidades de Registro

La EC-GENCAT autentica, previamente a la emisión y entrega de un certificado CIPISR, para cualquiera de los componentes de una Entidad de Registro, la identidad de la Entidad de Registro y del operador conforme a la sección correspondiente de la presente DPC.

3.2.2.3 Suscriptores de Certificados

No se requiere realizar procedimiento de autenticación de la organización titular del certificado puesto que se trata de certificados corporativos, en los que la organización suscriptora del certificado i la Entidad de Registro coinciden.

3.2.3. Autenticación de la identidad de una persona física

Esta sección contiene informaciones para la comprobación de la identidad de una persona física identificada en un certificado.

3.2.3.1. Elementos de identificación

El número y tipo de documentos necesarios para acreditar la identidad del poseedor de claves son los que admite cada organización suscriptora tal como se recoge en su normativa reguladora.

En todo caso, estos documentos identificativos contendrán como mínimo:

- Nombre y apellidos de la persona
- Número de identidad reconocido legalmente (DNI, NIF o NIE de los países firmantes del Acuerdo de Schengen; pasaporte en el caso de los certificados de extranjero).
- Fecha y lugar de nacimiento
- Cualquier otra información que pueda ser utilizada para diferenciar a una persona de la otra, dentro del ámbito de la Institución (por ejemplo: fotografía, correo-e, categoría, cargo, etc.).

3.2.3.2. Validación de los elementos de identificación

Sin estipulación adicional.

3.2.3.3. Necesidad de presencia personal

Sin estipulación adicional.

3.2.3.4. Vinculación de la persona física con la organización

- Requisitos para certificados de clase 1

Como se trata de certificados corporativos, en que la Entidad de Registro y el suscriptor coinciden, no es necesario obtener una justificación documental específica de la vinculación del poseedor de la clave con la Entidad de Registro, sino que se utilizan los registros internos de la Institución.

- Requisitos para certificados de clase 2

La EC-GENCAT tiene que obtener una justificación documental de la vinculación de la persona física con la organización, mediante cualquier medio admitido en derecho.

La EC-GENCAT puede utilizar Entidades de Registro para esta tarea.

3.2.4. Información no verificada

La EC-GENCAT se responsabiliza de que toda la información incluida en la solicitud del certificado sea exacta y completa para la finalidad del certificado; y detiene derecho a su uso (por ejemplo derecho a utilizar cierto nombre en la dirección de correo electrónico o la legitimidad en el empleo de un servidor web).

No obstante lo anterior, los certificados pueden incluir información no verificada, como por ejemplo, la dirección de correo electrónico, siempre que se indique a los usuarios finales en el propio certificado o en los instrumentos jurídicos correspondientes.

3.3. Identificación y autenticación de solicitudes de renovación

3.3.1. Validación para la renovación de certificados

Antes de renovar un certificado, la entidad de Certificación tendrá que comprobar –mediante la intervención de una Entidad de Registro- que la información utilizada para verificar la identidad y el resto de datos del suscriptor y del poseedor de la clave continúan siendo válidas.

Si cualquier información del suscriptor o del poseedor de la clave ha cambiado, se registrará adecuadamente la nueva información, de acuerdo con lo establecido en la sección correspondiente.

3.3.2. Validación para la renovación de certificados después de la revocación

La renovación de certificados después de la revocación no es posible.

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

Nota: el término “notificación” se utiliza en este documento como equivalente de “comunicación”, a excepción de las tramitaciones documentales con otros organismos públicos exigibles por la legislación aplicable.

4.1 Solicitud de emisión de certificado

4.1.1 Legitimación para solicitar la emisión

4.1.1.1 Requisitos generales

Únicamente pueden solicitar certificados de infraestructura las Entidades de Certificación Vinculadas a la jerarquía pública de certificación de Catalunya, operada por el Consorci AOC.

4.1.1.2 Requisitos específicos para el Certificado CIC

La futura Entidad de Certificación no podrá solicitar el Certificado CIC hasta que no haya completado su procedimiento de admisión, en la Jerarquía de Entidades de Certificación de l Consorci AOC.

4.1.2 Procedimiento de alta; Responsabilidades

La EC-GENCAT, con carácter previo a la emisión de un certificado, se asegura de que las solicitudes de certificados son completas, precisas y están debidamente autorizadas.

Antes de la emisión y entrega de un certificado, la EC-GENCAT informará al suscriptor o, en su caso, al poseedor de claves de los términos y condiciones aplicables al certificado. Este requisito se cumple mediante la entrega del instrumento jurídico que vincula la EC-GENCAT con el suscriptor o de la hoja de entrega al poseedor de claves, en la que se incluirá dicha información. Dicha información se comunicará en soporte perdurable, en papel o electrónicamente, y en lenguaje fácilmente comprensible.

4.2 Procesamiento de la solicitud de certificación

4.2.1 Requisitos para todo tipo de certificados

Una vez ha tenido lugar una petición de certificado, la EC-GENCAT, a través de una persona autorizada, verifica la información proporcionada, conforme a los requisitos previstos en la presente DPC.

- Si la verificación no es correcta, la EC-GENCAT deniega la petición. En el supuesto de que las irregularidades no puedan corregirse, la EC-GENCAT deniega la solicitud definitivamente.
- Si la verificación es correcta, la EC-GENCAT:

- Aprueba la solicitud.
- Genera, en su caso, el par de claves y el certificado.

4.2.2 Requisitos adicionales para el Certificado CIC

Cuando la Entidad de Certificación que solicita ser vinculada a la jerarquía pública de certificación de Catalunya no esté operada por el Consorci AOC, se comprobará, antes de emitir el certificado, que el prestador de servicios de certificación correspondiente pueda demostrar la necesaria fiabilidad de sus servicios.

La EC-GENCAT comprobará, en el proceso de admisión de la Entidad de Certificación, los siguientes aspectos:

- Que las políticas y procedimientos operados por la Entidad de Certificación no son discriminatorios.
- Que la Entidad de Certificación ofrecerá sus servicios a todos los solicitantes cuyas actividades entren en el ámbito de operación declarado en su DPC, de acuerdo con lo establecido en la sección 1.3 de la Política General de Certificación del Consorci AOC.
- Que la Entidad de Certificación es una entidad legal, de acuerdo con lo establecido en la sección 1.3.1 de la Política General de Certificación de Consorci AOC, dato que será autenticado de acuerdo con lo establecido en la sección correspondiente la Política General de Certificación del Consorci AOC.
- Que la Entidad de Certificación dispone de sistemas de gestión de la calidad y la seguridad adecuados para la prestación del servicio, dato que será comprobado en la auditoría de conformidad prevista en la sección 8 de la Política General de Certificación del Consorci AOC.
- Que la Entidad de Certificación utiliza personal calificado y con la experiencia necesaria para la prestación de los servicios ofrecidos, en el ámbito de la firma electrónica y los procedimientos adecuados de seguridad y de gestión.
- Que la Entidad de Certificación cumple los requisitos de capacidad financiera establecidos en la sección 9.2 de la Política General de Certificación del Consorci AOC.
- Que la Entidad de Certificación cumple los requisitos relativos a los procedimientos de resolución de disputas, establecidos en la sección 9.13 de la Política General de Certificación del Consorci AOC.
- Que la Entidad de Certificación ha documentado adecuadamente las relaciones jurídicas en virtud de las que externaliza parte o la totalidad de sus servicios.

4.3 Emisión de certificado

4.3.1 Acciones de la EC-GENCAT durante el proceso de emisión

Para cada solicitud de certificado tramitada, la EC-GENCAT:

- Utiliza un procedimiento de generación de certificados X.509 v3 que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada, mediante la firma digital de la EC-GENCAT.
- Protege la confidencialidad y la integridad de los datos de registro.

- Incluye en los certificados personales las informaciones establecidas en el artículo. 11.2 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, de acuerdo con lo establecido en la sección 3 de la presente DPC.
- Cumple las obligaciones establecidas por los artículos 12, 18, 19, 20 y otros aplicables, de la Ley 59/2003, de 19 de diciembre, de firma electrónica, en la generación de certificados reconocidos.
- Cumple los controles establecidos por esta declaración de prácticas de certificación.

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

4.3.2 Notificación de la emisión al suscriptor

La EC-GENCAT notifica al Consorci AOC la emisión del certificado, o la incidencia correspondiente. Asimismo, se indicará la disponibilidad del certificado y la forma de obtenerlo.

4.4 Aceptación del certificado

4.4.1 Responsabilidades del Prestador de Servicios de Certificación

La EC-GENCAT:

- Si no lo ha hecho antes, y cuando resulte necesario, acreditará la identidad del suscriptor.

- Proporcionará al suscriptor acceso al certificado.

- Entregará, en su caso, el dispositivo criptográfico de firma, verificación de firma, cifrado o descifrado.

- Proporcionará la siguiente información:

  - Información básica sobre la política y uso del certificado, incluyendo especialmente información sobre la Entidad de Certificación Vinculada y de la Declaración de Prácticas de Certificación aplicable, así como sus obligaciones, facultades y responsabilidades.
  - Información sobre el certificado y el dispositivo criptográfico.
  - Reconocimiento del poseedor de recibir el certificado y, en su caso, el dispositivo criptográfico, y aceptación de dichos elementos.
  - Obligaciones del poseedor de claves.
  - Responsabilidad de poseedor de claves.
  - Método de imputación exclusiva al poseedor de su clave privada y de sus datos de activación del certificado y, en su caso, del dispositivo criptográfico, de acuerdo con lo establecido en las secciones correspondientes de esta política.
  - La fecha del acto de entrega y aceptación.

4.4.2 Conducta que constituye aceptación del certificado

El certificado se puede aceptar mediante la firma de la hoja de poseedor o responsable de la custodia de claves.

También se puede aceptar el certificado mediante un mecanismo telemático de activación del certificado.

4.4.3 Publicación del certificado

Los certificados se pueden publicar sin el consentimiento previo de los poseedores de claves.

4.4.4 Notificación de la emisión a terceros

No aplicable.

4.5 Uso del par de claves y del certificado

4.5.1 Uso por los poseedores de claves

Sin estipulación adicional.

4.5.1.1 Requisitos adicionales para los certificados CIC

Los certificados CIC sólo pueden ser utilizados para funciones de Entidad de Certificación, en conjunción con un dispositivo seguro de generación de firma, de acuerdo con los requisitos establecidos en la Política General de Certificación del Consorci AOC.

4.5.2 Uso por el tercero que confía en certificados

Sin estipulación adicional.

4.6 Renovación de certificados sin renovación de claves

No se permite la renovación de certificados sin renovación de claves.

4.7 Renovación de certificados con renovación de claves

Sin estipulación adicional.

4.8 Renovación telemática

Sin estipulación adicional.

4.9 Modificación de certificados

Sin estipulación adicional.

4.10 Revocación y suspensión de certificados

4.10.1 Causas de revocación de certificados

Sin estipulación adicional.

4.10.2 Legitimación para solicitar la revocación

Sin estipulación adicional.

4.10.3 Procedimientos de solicitud de revocación

La solicitud de revocación debe ser entregada personalmente, enviada por correo electrónico firmado o por correo certificado convencional. Debe incluirse la información suficiente para poder identificar razonablemente, a criterio de la EC-GENCAT, por un lado, el certificado que se solicita revocar y, por otra parte, la autenticidad y autoridad del solicitante.

Esta información suficiente debe estar compuesta por los datos de contacto del poseedor de claves incluido su DNI o equivalente, y de la entidad que pide la revocación, la fecha y la razón de la petición, así como el número de serie del certificado.

Quien haga la solicitud de revocación puede pedir a la Entidad de Registro más información sobre este procedimiento.

La petición de revocación con la documentación necesaria es recogida, registrada y notificada por la Entidad de Registro.

Las Entidades de Registro atienden las solicitudes de revocación dentro de su horario de oficina. Fuera de este horario, cuando sea urgente dejar sin efecto un certificado, se puede solicitar la suspensión cautelar del certificado mediante un allamada telefónica al Centro de Atención al Usuario del Consorci AOC, cuyo horario es 24x365.

La acción de revocación la lleva a cabo uno de los operarios de laEntidad de Registro, quien accede a la aplicación web al efecto, autenticándose mediante un certificado de operador (CIPISR), de clase 1 si es operador de la Entidad de Registro o de clase 2 cuando sea un operador del Centro de Atención al Usuario) emitido por la EC-GENCAT.

Una vez registrado el cambio de estado del certificado en el sistema de la EC-GENCAT, de forma automàtica y en la mayor brevedad posible, se genera y publica una nueva Lista de Certificados Revocados (LCR o CRL) en la cual constarà la referecia de este certificado.

Se informa al suscriptor y, en su caso, al poseedor de claves, sobre el cambio de estado del certificado, de acuerdo con el artículo 10.2 de la Ley de firma electrónica.

4.10.4 Periodo temporal de solicitud de revocación

Sin estipulación adicional

4.10.5 Periodo máximo de procesamiento de la solicitud de revocación

Sin estipulación adicional.

4.10.6 Obligación de consulta de información de revocación de certificados

Los verificadores comprueban el estado de aquellos certificados en los que desean confiar.

Un método por el que se verifica el estado de los certificados es consultando la lista de revocación de certificados o LRC más reciente emitida por la EC-GENCAT.

La EC-GENCAT suministra información a los verificadores sobre cómo y dónde encontrar la LRC correspondiente.

4.10.7 Frecuencia de emisión de listas de revocación de certificados (LRCs)

Sin estipulación adicional.

4.10.8 Periodo máximo de publicación de LRCs

Sin estipulación adicional.

4.10.9 Disponibilidad de servicios de comprobación de estado de certificados

Sin estipulación adicional.

4.10.10 Obligación de consulta de servicios de comprobación de estado de certificados

Sin estipulación adicional.

4.10.11 Otras formas de información de revocación de certificados

Sin estipulación adicional.

4.10.12 Procedimientos especiales en caso de compromiso de la clave privada

Sin estipulación adicional.

4.10.13 Causas de suspensión de certificados

Sin estipulación adicional.

4.10.14 Quien puede solicitar la suspensión

Sin estipulación adicional.

4.10.15 Procedimientos de petición de suspensión

Sin estipulación adicional.

4.10.16 Período máximo de suspensión

Sin estipulación adicional.

4.10.17 Habilitación de un certificado suspendido

Sin estipulación adicional.

4.11 Servicios de comprobación de estado de certificados

4.11.1 Características de operación de los servicios

Las LCR se publican en la webdel Consorci AOC y en las URLs indicadas en los certificados emitidos.

De forma alternativa, los verificadores podrán consultar los certificados publicados en el directorio de la EC-GENCAT.

4.11.2 Disponibilidad de los servicios

Los verificadores de certificados digitales pueden consultar un servicio en linea que responda sobre el estado de certificados (servicio *OCSP responder* u otros servicios de validación de certificados) operado por un prestador de servicios de validación en el que se confía.

El Consori AOC ofrece de manera gratuïta un servicio *OCSP responder* para la comprobación en línea del estado de los certificados emitidos por las Entidades de Certificación que integran la jerarquía pública de certificación de Cataluña.

La URL en la que se encuentra disponible dicho servicio se indica en el contenido de los certificados emitidos. La información relativa al perfil OCSP y, en general, al funcionamiento del servicio, se puede encontrar en http://www.aoc.cat/catcert .

4.11.3 Otras funciones de los servicios

Sin estipulación adicional.

4.12 Finalización de la suscripción

Sin estipulación adicional.

4.13 Depósito y recuperación de claves

4.13.1 Política y prácticas de depósito y recuperación de claves

No se practica recuperación de.

4.13.2 Política y prácticas de encapsulamiento y recuperación de claves de sesión

Sin estipulación adicional.

5. Controles de seguridad física, de gestión y de operaciones

Sin estipulación adicional.

5.1 Controles de seguridad física

5.1.1 Localización y construcción de las instalaciones

Sin estipulación adicional.

5.1.2 Acceso físico

Sin estipulación adicional.

5.1.3 Electricidad y aire acondicionado

Sin estipulación adicional.

5.1.4 Exposición al agua

Sin estipulación adicional.

5.1.5 Advertencia y protección de incendios

Sin estipulación adicional.

5.1.6 Almacenaje de soportes

Sin estipulación adicional.

5.1.7 Tratamiento de residuos

Sin estipulación adicional.

5.1.8 Copia de seguridad fuera de las instalaciones

Sin estipulación adicional.

5.2 Controles de procedimientos

La EC-GENCAT garantiza que sus sistemas se operan de forma segura, y por esto establece e implanta procedimientos para las funciones que afecten a la provisión de sus servicios.

El personal al servicio de la EC-GENCAT realiza los procedimientos administrativos y de gestión de acuerdo con la política de seguridad de la EC-GENCAT.

5.2.1 Funciones fiables

Sin estipulación adicional.

5.2.2 Número de personas por tarea

Sin estipulación adicional.

5.2.3 Identificación y autenticación para cada función

Sin estipulación adicional.

5.2.4 Roles que requieren separación de tareas

Sin estipulación adicional.

5.3 Controles de personal

La EC-GENCAT tiene en cuenta los siguientes aspectos:

- Se mantiene confidencialidad de la información, poniendo los medios necesarios y manteniendo una actitud adecuada en el desarrollo de sus funciones dentro y fuera del ámbito laboral en lo referente a la seguridad de las infraestructuras.
- Se es diligente y responsable en el tratamiento, mantenimiento y custodia de los activos de la infraestructura identificados en la política, en los planes de seguridad o en este documento.
- No se revela información no pública fuera del ámbito de la infraestructura, ni se extraen soportes de información a niveles de seguridad inferiores.

- Se reporta al Responsable de Seguridad, lo mejor posible, cualquier incidente que se considere que afecta a la seguridad de la infraestructura, o limitar la calidad del servicio.
- Se utilizan los activos de la infraestructura para las finalidades que les han sido encomendadas.
- Se exigen manuales o guías de usuario de los sistemas que utiliza, que permiten desarrollar su función correctamente.
- Se exige documentación escrita que marque sus funciones y medidas de seguridad a que está sometido.
- El responsable de seguridad vela porque el punto anterior sea ejecutado, proveyendo a los responsables de área toda la información que fuera necesaria.
- No se instalan en ninguno de los sistemas de la infraestructura, software o hardware que no sea expresamente autorizado por escrito por el responsable de sistemas de información.
- No se accede voluntariamente, ni se elimina o altera información no destinada a su persona o perfil profesional.

El personal afectado por esta normativa es:

- el Responsable del Servicio.
- el Responsable de la EC-GENCAT.
- el Responsable de Seguridad.
- el Responsable de Operaciones.
- el Operador de Ceremonias de Claves.
- el Equipo técnico de administración, operación y explotación.
- los Administradores de la Red, y
- los Usuarios de laEC-GENCAT.

Además, se ve afectado el siguiente personal del Consorci AOC:

- quien hace las peticiones de los certificados.
- quien hace la aprobación y validación de las peticiones de certificados.
- quien hace la generación / personalización de certificados.
- quien custodia las claves o tokens criptográficos.
- quien custodia las llaves o combinaciones de seguridad de acceso a la sala de operaciones.
- quien accede a información clasificada.
- el personal de comunicaciones y operaciones.
- el personal de seguridad (física y lógica) involucrados en la operación.
- el responsable del servicio.

5.3.1 Requisitos de historial, calificaciones, experiencia y autorización

Sin estipulación adicional.

5.3.2 Requisitos de formación

Sin estipulación adicional.

5.3.3 Requisitos y frecuencia de actualización formativa

Sin estipulación adicional.

5.3.4 Secuencia y frecuencia de rotación laboral

Sin estipulación adicional.

5.3.5 Sanciones por acciones no autorizadas

Sin estipulación adicional.

5.3.6 Requisitos de contratación de profesionales

Sin estipulación adicional.

5.3.7 Suministro de documentación al personal

Sin estipulación adicional.

5.4 Procedimientos de auditoría de seguridad

5.4.1 Tipos de acontecimientos registrados

Sin estipulación adicional.

-

5.4.2 Frecuencia de tratamiento de registros de auditoría

Sin estipulación adicional.

5.4.3 Periodo de conservación de registros de auditoría

Sin estipulación adicional.

5.4.4 Protección de los registros de auditoría

Sin estipulación adicional.

5.4.5 Procedimientos de generación de copias de seguridad

- Sin estipulación adicional.

5.4.6 Localización del sistema de acumulación de registros de auditoría

Sin estipulación adicional.

5.4.7 Notificación del acontecimiento de auditoría al causante del acontecimiento

Sin estipulación adicional.

5.4.8 Análisis de vulnerabilidades

Sin estipulación adicional.

5.5 Archivo de informaciones

Sin estipulación adicional.

5.5.1 Tipos de acontecimientos registrados

- Sin estipulación adicional.

5.5.2 Periodo de conservación de registros

La EC-GENCAT guarda los registros especificados en la sección 5.5.1 de la presente DPC durante 15 años, contados desde el momento de la expedición del certificado. Toda la información relativa a los Certificados de Infraestructura de Certificación se guarda de forma permanente.

L'EC-GENCAT guarda los registros especificados en la sección 5.5.1 en relación con los certificados Extended Validation por un periodo de 7 años, contados desde el momento de emisión del certificado.

5.5.3 Protección del archivo

- Sin estipulación adicional.

5.5.4 Procedimientos de generación de copias de seguridad

Sin estipulación adicional.

5.5.5 Requisitos de sellado de cautela de fecha y hora

Sin estipulación adicional.

5.5.6 Localización del sistema de archivo

Sin estipulación adicional.

5.5.7 Procedimientos de obtención y verificación de información de archivo

Sin estipulación adicional.

5.6 Renovación de claves

Los certificados de la EC-GENCAT que se hayan renovado, se comunican a los usuarios finales, mediante su publicación en la pàgina web del Servei de Certificació Digital del Consorci AOC.

5.7 Compromiso de claves y recuperación de desastre

5.7.1 Procedimiento de gestión de incidencias y compromisos

La EC-GENCAT establece los procedimientos que aplica en la gestión de las incidencias que afectan sus claves y, muy especialmente, en los compromisos de la seguridad de las claves.

5.7.2 Corrupción de recursos, aplicaciones o datos

Cuando tenga lugar un acontecimiento de corrupción de recursos, aplicaciones o datos la EC-GENCAT inicia las gestiones necesarias, según los documentos Plan de Seguridad, Plan de Emergencia y Plan de Auditoría, para hacer que el sistema vuelva a su estado normal de funcionamiento.

5.7.3 Compromiso de la clave privada de la Entidad

El plan de continuidad de negocio de la EC-GENCAT (o plan de recuperación de desastres) considera el compromiso o la sospecha de compromiso de la clave privada de la EC-GENCAT como un desastre.

En caso de compromiso la EC-GENCAT:

- Informa a todos los suscriptores y verificadores del compromiso.
- Indica que los certificados y la información del estado de revocación entregados usando la clave de la EC-GENCAT ya no son válidos.

5.7.4 Desastre sobre las instalaciones

La EC-GENCAT desarrolla, mantiene, prueba y, si es necesario, ejecuta un plan de emergencia en el caso de desastre, ya sea por causas naturales o causado por el hombre, sobre las instalaciones, que indica cómo se restauran los servicios de los Sistemas de Información. La ubicación de los sistemas de recuperación de desastre dispone de las protecciones físicas de seguridad detalladas en el Plan de Seguridad.

La EC-GENCAT es capaz de restaurar la operación normal de la PKI en las 24 horas siguientes al desastre, pudiendo, como mínimo, ejecutarse las siguientes acciones:

- Revocación de certificados (excepto en el mes de agosto).
- Publicación de información de revocación.

La base de datos de recuperación de desastres utilizada por la EC-GENCAT está sincronizada con la base de datos de producción, dentro de los límites temporales especificados en el Plan de Seguridad. Los equipos de recuperación de desastres de la EC-GENCAT tienen las medidas de seguridad físicas especificadas en el Plan de Seguridad.

5.8 Finalización del servicio

5.8.1 EC-GENCAT

Sin estipulación adicional.

5.8.2 Entidad de Registro

Sin estipulación adicional.

6. Controles de seguridad técnica

La EC-GENCAT utiliza sistemas y productos fiables, que están protegidos contra toda alteración y que garantizan la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte.

6.1 Generación e instalación del par de claves

6.1.1 Generación del par de claves

6.1.1.1 Requisitos para todos los certificados

Las claves pública y privada de los certificados podrán ser generadas por el futuro suscriptor o por la EC-GENCAT.

6.1.2 Envío de la clave privada al suscriptor

Sense estipulació addicional.

6.1.3 Envío de la clave pública al emisor del certificado

Sense estipulació addicional.

6.1.4 Distribución de la clave pública del Prestador de Servicios de Certificación

La clave de la EC-GENCAT y las claves de las Entidades de Certificación anteriores en la jerarquía pública de certificación de Catalunya son comunicadas a los verificadores, asegurando la integridad de la clave y autenticando el origen.

La clave pública de la EC-ACC (Entidad de Certificación del Consorci AOC) que es la raíz de la jerarquía, se publica en el Directorio de la EC-GENCAT, en forma de certificado auto firmado, junto a una declaración referente a que la clave permite autenticar a la EC-GENCAT.

Se establecen medidas adicionales para confiar en el certificado auto firmado, tal como la comprobación de la huella digital del certificado.

La clave pública de la EC-GENCAT se publica en el Directorio de la EC-GENCAT, en forma de certificado CIC firmado por el Consorci AOC.

Los usuarios acceden al Directorio para obtener las claves públicas de la EC-GENCAT.

6.1.5 Medidas de claves

Las claves de la EC-GENCAT son al menos de 2.048 bits.

Las claves de todos los certificados emitidos por la EC-GENCAT son de 2.048 bits.

6.1.6 Generación de parámetros de clave pública

Sin estipulación adicional.

6.1.7 Comprobación de calidad de parámetros de clave pública

Sin estipulación adicional.

6.1.8 Generación de claves en aplicaciones informáticas o en bienes de equipo

Sin estipulación adicional.

6.1.9 Propósitos de uso de claves

La EC-GENCAT incluye la extensión *KeyUsage* en todos los certificados, indicando los usos permitidos de las correspondientes claves privadas.

6.2 Protección de la clave privada

6.2.1 Estándares de módulos criptográficos

6.2.1.1.Estándares de los módulos criptográficos

Sin estipulación adicional.

6.2.1.2.Ciclo de vida de las tarjetas con circuito integrado

Sin estipulación adicional.

6.2.2 Control por más de una persona (n de m) sobre la clave privada

Sin estipulación adicional.

6.2.3 Depósito de la clave privada

Sin estipulación adicional.

6.2.4 Copia de seguridad de la clave privada

Sin estipulación adicional.

6.2.5 Archivo de la clave privada

Sin estipulación adicional.

6.2.6 Introducción de la clave privada en el módulo criptográfico

Sin estipulación adicional.

6.2.7 Almacenaje de la clave privada en el módulo criptográfico

Sin estipulación adicional.

6.2.8 Método de activación de la clave privada.

Se requieren al menos dos personas para activar la clave privada de la EC-GENCAT.

Para certificados CIPISR, la clave privada del suscriptor se activa mediante la introducción del PIN en la tarjeta inteligente o dispositivo criptográfico.

6.2.9 Método de desactivación de la clave privada

Sin estipulación adicional.

6.2.10 Método de destrucción de la clave privada

Sin estipulación adicional.

6.2.11 Clasificación de los módulos criptográficos

Sin estipulación adicional.

6.3 Otros aspectos de gestión del par de claves

6.3.1 Archivo de la clave pública

La EC-GENCAT archiva sus claves públicas, de acuerdo con lo establecido en la sección 5.5 de la presente DPC.

6.3.2 Periodos de utilización de las claves pública y privada

Sin estipulación adicional.

6.4 Datos de activación

6.4.1 Generación e instalación de los datos de activación

Sin estipulación adicional.

6.4.2 Protección de datos de activación

6.4.2.1 Para certificados CIPISR

Sin estipulación adicional.

6.4.3 Otros aspectos de los datos de activación

Sin estipulación adicional.

6.5 Controles de seguridad informática

6.5.1 Requisitos técnicos específicos de seguridad informática

Sin estipulación adicional.

-

6.5.2 Evaluación del nivel de seguridad informática

Las aplicaciones de EC y ER son fiables, de acuerdo con la especificación técnica CEN CWA 14167-1, evaluándose el grado de cumplimiento mediante una auditoria de seguridad informática conforme a la especificación técnica CWA 14172-3 y un perfil de protección adecuado, de acuerdo con la norma ISO 15408 o equivalente.

6.6 Controles técnicos del ciclo de vida

6.6.1 Controles de desarrollo de sistemas

Sin estipulación adicional.

6.6.2 Controles de gestión de seguridad

Sin estipulación adicional.

6.6.3 Evaluación del nivel de seguridad del ciclo de vida

Sin estipulación adicional.

6.7 Controles de seguridad de red

Se garantiza que el acceso a las diferentes redes de la EC-GENCAT es limitado a individuos debidamente autorizados. En particular:

- Se implementan controles (como por ejemplo cortafuegos) para proteger la red interna de dominios externos accesibles por terceras partes. Los cortafuegos se configuran de forma que se impidan accesos y protocolos que no sean necesarios para la operación de la EC-GENCAT.
- Los datos sensibles se protegen cuando se intercambian a través de redes no seguras (incluyendo los datos de registro del suscriptor).
- Se garantiza que los componentes locales de red (como direccionadores) se encuentran ubicados en entornos seguros, así como la auditoría periódica de sus configuraciones.

6.8 Sello de tiempo

Sin estipulación adicional.

7. Perfiles de certificados y listas de certificados revocados

7.1 Perfil de certificado

Sin estipulación adicional.

Los documentos descriptivos de los diferentes perfiles de dertificados digitales que emite la EC-GENCAT se publican en la web del Consorci AOC.

7.2 Perfil de la lista de revocación de certificados

Sin estipulación adicional.

8. Auditoría de conformidad

La EC-GENCAT realiza periódicamente una auditoría de conformidad para probar que cumple los requisitos de seguridad y de operación necesarios para formar parte de la jerarquía pública de certificación de Catalunya.

La EC-GENCAT puede delegar la ejecución de las auditorías en una tercera entidad contratada por el Consorci AOC. En este caso la EC-GENCAT coopera completamente con el personal que lleva a término la investigación.

8.1 Frecuencia de la auditoría de conformidad

Sin estipulación adicional.

8.2 Identificación y calificación del auditor

LaEC-GENCATacude a auditores independientes externo, el cual tiene que demostrar experiencia en seguridad informática, en seguridad de Sistemas de Información y en auditorías de conformidad de Autoridades de Certificación y los elementos relacionados.

8.3 Relación del auditor con la entidad auditada

Las auditorías externas de conformidad ejecutadas por terceros están realizadas por una entidad independiente de la EC-GENCAT.

8.4 Relación de elementos objeto de auditoría

Sin estipulación adicional.

8.5 Acciones a emprender como resultado de una falta de conformidad

Sense estipulació addicional.

8.6 Tratamiento de los informes de auditoría

Los informes de resultados de las auditorias serán entregados al Consorci AOC en tanto que Prestador de Servicios de Certificación, en un plazo máximo de 15 días después de la ejecución de la auditoría, para su evaluación y gestión diligente.

9. Requisitos comerciales y legales

9.1 Tarifas

9.1.1 Tarifa de emisión o renovación de certificados

El Consorci AOC establece las tarifas que aplica la EC-GENCAT, en la prestación de sus servicios. Las tarifas se pueden consultar en la web del servicio de certificación digital del Consorci AOC

9.1.2 Tarifa de acceso a certificados

No se puede establecer una tarifa por el acceso a los certificados.

9.1.3 Tarifa de acceso a información de estado de certificado

No se puede establecer una tarifa por el acceso a la información de acceso a los certificados.

9.1.4 Tarifas de otros servicios

Sin estipulación adicional

9.1.5 Política de reintegro

El Consorci AOCno practicará reembolsos. En caso de productos defectuosos se procederá a sustituir el producto defectuoso por otro en buen estado.

9.2 Capacidad financiera

9.2.1 Seguro de responsabilidad civil

El Consorci AOCdispone de una garantía de cobertura de su responsabilidad civil suficiente, en los términos previstos en el artículo 20.2 de la Ley 59/2003, de 19 de diciembre, excepto cuando se encuentre eximida por Ley de esta obligación. Este seguro cubre las actuaciones del Consorci AOC como prestador de servicios de certificación.

9.2.2 Otros activos

Sin estipulación adicional.

9.2.3 Cobertura de aseguramiento para suscriptores y terceros que confíen en certificados

La cobertura la aporta el seguro previsto en el apartado 9.2.1, por los daños previstos por la Ley 59/2003, de 19 de diciembre, excluidas las exoneraciones legales de responsabilidad que prevé su artículo 23.

9.3 Confidencialidad

9.3.1 Informaciones confidenciales

Sin estipulación adicional.

9.3.2 Informaciones no confidenciales

Sin estipulación adicional.

9.3.3 Responsabilidad para la protección de información confidencial

Sin estipulación adicional.

9.4 Protección de datos personales

9.4.1 Política de Protección de Datos Personales

Sin estipulación adicional.

9.4.2 Datos de carácter personal no disponibles a terceros

Sin estipulación adicional.

9.4.3 Datos de carácter personal disponibles a terceros

Sin estipulación adicional.

9.4.4 Responsabilidad correspondiente a la protección de los datos personales

Sin estipulación adicional.

9.4.5 Gestión de incidencias relacionadas con los datos de carácter personal

Sin estipulación adicional.

9.4.6 Prestación del consentimiento en el uso de los datos personales

Sin estipulación adicional.

9.4.7 Comunicación de datos personales

Sin estipulación adicional.

9.5 Derechos de propiedad intelectual

9.5.1 Propiedad de los certificados e información de revocación

Sin estipulación adicional.

9.5.2 Propiedad de la política de certificado y Declaración de Prácticas de Certificación

Sin estipulación adicional

9.5.3 Propiedad de la información relativa a nombres

Sin estipulación adicional.

9.5.4 Propiedad de claves

Sin estipulación adicional..

9.6 Obligaciones y responsabilidad civil

9.6.1 Entidades de Certificación

9.6.1.1 Obligaciones generales de la EC-GENCAT

- Sin estipulación adicional.

9.6.1.2 Garantías ofrecidas a suscriptores y verificadores

Sin estipulación adicional.

9.6.2 Entidades de Registro

9.6.2.1 Obligaciones y otros compromisos

Sin estipulación adicional, exceptuando la obligación de almacenar las hojas de entrega del certificado durante un periodo de 15 años, que es asumida por las entidades suscriptoras de los certificados corporativos que emite la EC-GENCAT

En cuanto al número de operadores de la autoridad de registro que tiene que nombrar para la EC-GENCAT tendrán que ser cuatro o más los empleados que trabajen para ella.

a.

9.6.3 Garantías ofrecidas a suscriptores y verificadores

9.6.3.1 Garantía del Consorci AOC por los servicios de certificación digital

9.6.3.2 Exclusión de la garantía

Sin estipulación adicional

9.6.4 Suscriptores

9.6.4.1 Obligaciones y otros compromisos

Sin estipulación adicional

9.6.4.2 Garantías ofrecidas por el suscriptor

Sin estipulación adicional

9.6.4.3 Protección de la clave privada

Sin estipulación adicional.

9.6.5 Verificadores

9.6.5.1 Obligaciones y compromisos

Sin estipulación adicional.

9.6.5.2 Garantías ofrecidas por el verificador

Sin estipulación adicional

9.6.6 Otros participantes

9.6.6.1 Obligaciones y garantías del directorio

Sin estipulación adicional

9.6.6.2 Garantías ofrecidas por el directorio

La EC-GENCAT tiene la responsabilidad civil del directorio de certificación.

9.7 Renuncias de garantías

9.7.1 Rechazo de garantías de la EC-GENCAT

La EC-GENCAT puede rechazar todas las garantías del servicio, que no se encuentren vinculadas a obligaciones establecidas por la Ley 59/2003, de 19 de diciembre, de firma electrónica, incluyendo especialmente la garantía de adaptación para un propósito particular o garantía de uso mercantil del certificado.

9.8 Limitaciones de responsabilidad

9.8.1 Limitaciones de responsabilidad de la EC-GENCAT

La EC-GENCAT limita su responsabilidad restringiendo el servicio a la emisión y gestión de certificados y, en su caso, de pares de claves de suscriptores y depósitos criptográficos (de firma y verificación de firma, así como de cifrado o descifrado) subministrados por ésta.

La EC-GENCAT puede limitar su responsabilidad mediante la inclusión de límites de uso del certificado, y límites de valor de las transacciones para las que puede utilizarse el certificado.

9.8.2 Caso fortuito y fuerza mayor

La EC-GENCAT incluye cláusulas para limitar su responsabilidad en caso fortuito y en caso de fuerza mayor, en los instrumentos jurídicos con los que vincule suscriptores y verificadores.

9.9 Indemnizaciones

9.9.1 Cláusula de indemnidad de suscriptor

No se establecerá cláusula de indemnidad del suscriptor.

9.9.2 Cláusula de indemnidad de verificador

No se establecerá cláusula de indemnidad del verificador.

9.10 Plazo y finalización

9.10.1 Plazo

La EC-GENCAT establece, en sus instrumentos jurídicos con los suscriptores y los verificadores, una cláusula que determina el período de vigencia de la relación jurídica en virtud de la que suministra certificados a los suscriptores.

9.10.2 Finalización

La EC-GENCAT establece, en sus instrumentos jurídicos con los suscriptores y los verificadores, una cláusula que determina las consecuencias de la finalización de la relación jurídica en virtud de la que suministra certificados a los suscriptores.

9.10.3 Supervivencia

Sin estipulación adicional

.

9.11 Notificaciones

Sin estipulación adicional.

9.12 Modificaciones

9.12.1 Procedimiento para las modificaciones

9.12.2 Sin estipulación adicional.Periodo y mecanismos para notificaciones

Las modificaciones deeste documento serán aprobadas por el Consorci AOC, conforme se establece en el apartado 1.5.

9.12.3 Circunstancias en las que un OID tiene que ser cambiado

Sin estipulación adicional.

9.13 Resolución de conflictos

9.13.1 Resolución extrajudicial de conflictos

Sin estipulación adicional.

9.13.2 Jurisdicción competente

Sin estipulación adicional.

9.14 Ley aplicable

Sin estipulación adicional.

9.15 Conformidad con la ley aplicable

La EC-GENCAT manifiesta, en este documento y en los instrumentos jurídicos con suscriptores, el cumplimiento de la Ley 59/2003, de 19 de diciembre, de firma electrónica. La prestación de servicios se ajusta a la legislación vigente, en especial, la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y comercio electrónico.

9.16 Cláusulas diversas

9.16.1 Acuerdo íntegro

Sin estipulación adicional.

9.16.2 Subrogación

Sin estipulación adicional.

9.16.3 Divisibilidad

Sin estipulación adicional.

9.16.4 Aplicaciones

Sin estipulación adicional.

9.16.5 Otras cláusulas

Sin estipulación adicional.

ANEXO – Control documental

Control de versiones DPC EC-GENCAT 1r semestre 2016

Proyecto:	**Informe modificación del documento DPC EC-GENCAT**
Entidad de destino:	**Consorci AOC**
Código de referencia:	**Revisión 1r semestre 2016**
Versión:	**Cambios de la v1.4 a la v2.0 en catalán y en castellano**
Fecha de la edición:	**05/08/2016**

Versión	Partes que cambian	Descripción del cambio	Autor del cambio	Fecha del cambio
2.0	Todas	Revisión parcial del documento – Cumplimiento WebTrust	Servei de Certificació Digital AOC	05/08/2016