Consorci
Administració Oberta
de Catalunya

Declaración de Prácticas de Certificación
Entidad de CertificaciónACC
(EC-ACC)

Referencia:	D1111_E0650_N-DPC EC-ACC
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 CertificaciónACC	
Fichero	D111 E0650 N-DPC EC-ACC 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 'Agencia Catalana de Certificación' (en adelante EC-ACC, 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-ACC.

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

1.1 Presentación

Cuando sedesarrolló 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 de CATCert (denominada EC-ACC) es la raíz de la jerarquía de confianza, y certifica las Entidades de Certificación que se crean dentro del marco de las administraciones públicas catalanas.

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.

En fecha 2 de agosto de 2011, el Gobierno de la Generalitat de Catalunya aprobó el acuerdo sobre medidas de racionalización y simplificación de la estructura del sector público de Catalunya, en el marco de las cuales se instaba a los departamentos competentes a formular e implantar estrategias de reordenación de su sector público que incidieran especialmente en la mejora de la eficiencia organizativa de la que cual se ha de derivar una eficiencia económica.

En esta línea, dentro de una larga lista de actuaciones que afectaban a un elevado número de entidades que integran el sector público de la Generalitat de Catalunya, se acordó promover las actuaciones necesarias para la integración de CATCert en el Consorcio AOC y proceder a la extinción de CATCert como organismo autónomo.

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 Agencia Catalana de Certificación en el Consorci AOC, en el cual revertiran todas las marcas, derechos, deberes y servicios gestionados hasta la fecha por CATCert.

La integración se hizo efectiva mediante 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-ACCha definido una tipología de servicios de certificación que permiten, a la EC-ACC, emitir 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.

LA EC-ACC 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.

Atendiendo al nivel de la Entidad de Certificación a la que se emite el Certificado CIC, se distinguen los siguientes tipos de Certificados:

a. Certificado de Infraestructura de Entidad de Certificación Raíz (CIC Raíz)

El Certificado CIC Raíz es el certificado que el Consorci AOC se expide de forma exclusiva a sí misma, como Entidad de Certificación Raíz de la Jerarquía pública de certificación de Cataluña, para emitir y gestionar los certificados de las Entidades de Certificación Vinculadas a dicha Jerarquía.

La duración de la licencia del CIC de la EC-ACC es de hasta treinta (30) años, a contar desde la fecha de su emisión.

b. Certificado de Infraestructura de Entidad de Certificación de nivel 1 (CIC-1)

El Certificado CIC-1 es el certificado que el Consorci AOC se expide de forma exclusiva a sí mismo como Entidad de Certificación intermedia de la Jerarquía pública de certificación de Catalunya para emitr y gestionar los certificados de las Entidades de Certificación Vinculadas a la citada Entidad de Certificación.

La duración de la licencia del CIC de los CIC de nivel 1 es de hasta veinticuatro (24) años, a contar desde la fecha de su emisión.

Entre las entidades de certificación vinculadas de nivel 1 se encuentra:

- La Entidad de Certificación de la Generalitat de Catalunya (EC-GENCAT) encargada de ofrecer soporte a la jerarquía pública de certificación de Catalunya en el ámbito del sector público de Catalunya a través de la EC-SAFP.

c. Certificado de Infraestructura de la Entidad de Certificación de nivel 2

La duración de la licencia de los CIC de nivel 2 es de hasta dieciséis (16) años, a contar desde la fecha de su emisión.

Entre las entidades de certificación vinculadas de nivel 2 se hallan:

- la Entidad de Certificación de la Generalitat de Catalunya (EC-GENCAT), encargada de ofrecer soporte a la jerarquía de certificación de Catalunya en el ámbito del sector público de Catalunya a través de la EC-SAFP.
- la Entidad de Certificación de la Administración Local (EC-AL), cuyos certificados se expiden al públicoal personal y a los dispositivos de los

Ayuntamientos, Consejos comarcales, Diputaciones, así como Organismos Autónomos y Empresas Públicas de los anteriores.

- la Entidad de Certificación de Universitats i Recerca (EC-UR), cuyos certificados se destinan al personal, a los estudiantes y a los dispositivos de las universidades y los centros de investigación de Catalunya, en su caso, conectados a la "Anella Científica".
- la Entidad de Certificación del Parlament de Catalunya (EC-Parlament), cuyos certificados se expiden a los Parlamentarios y el Personal de Administración y Servicios del Parlament de Catalunya, los Síndicos y el Personal de Administración y Servicios de la Sindicatura de Comptes, los Síndicos y el Personal de Administración y Servicios de la Sindicatura de Greuges, los dispositivos del Parlament de Catalunya; y el personal asesor de los partidos políticos o grupos parlamentarios dentro de la infraestructura del Parlament de Catalunya.
- la Entidad de Certificación del Sector Público (EC-SECTORPUBLIC), que se encarga de la prestación de servicios de certificación a la comunidad de usuarios de la Generalitat de Catalunya y el conjunto de las instituciones.
- la Entidad de Certificación Ciutadania (EC-Ciutadania), encargada dela prestación de servicios de certificación al conjunto de la ciudadanía.

d. Certificado de Infraestructura de la Entidad de Certificación de nivel 3

La duración de la licencia de los CIC de nivel 3 es de ocho (8) años, a contar desde la fecha de su emisión.

Actualmente, las entidades de certificación vinculadas de nivel 3 son:

- la Entidad de Certificación de la Secretaria d'Administració i Funció Pública (EC-SAFP), que expide certificados al personal y a los dispositivos de los Organismos, Departamentos y Empresas Públicas de la Administración de la Generalitat de Catalunya.
- la Entidad de Certificación de Universitat Rovira i Virgili (EC-URV), que expide certificados al personal, alos estudiantes y alos dispositivos de las facultades y los centros universitarios de la Universitat Rovira i Virgili.

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), que es utilizado por una entidad para firmar los sellos de tiempo que emite.

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-ACC.

La EC-ACCemite 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 Declaración de Prácticas de Certificación (DPC) incluye los procedimientos que aplica la EC-ACC 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-ACC”.

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

1.3.6.1.4.1.15096.1.2.2

1.2.2 Identificación de políticas de certificación cubiertas por esta DPC

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

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

  - Los CIC de nivel 0 se identifican con el identificador de objeto (OID): 1.3.6.1.4.1.15096.1.3.1.10.

    - **Certificado de Infraestructura de Entidad de Certificación Raíz (CIC Raíz)**

      El certificado CIC Raíz se identifica con el identificador de objeto (OID):1.3.6.1.4.1.15096.1.3.1.10.

  - Los CIC de nivel 1 se identifican con el identificador de objeto (OID): 1.3.6.1.4.1.15096.1.3.1.11.

    - **Certificado de Infraestructura de la Entidad de Certificación de la Generalitat de Catalunya (EC-GENCAT)**

      El certificado CIC de la EC-GENCAT es de nivel 1 y se identifica con el identificador de objeto (OID): 1.3.6.1.4.1.15096.1.3.1.11.

  - Los CIC de nivel 2 se 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.

- **Certificado de Infraestructura de la Entidad de Certificación de Ciudadanos (EC-idCAT)**

El certificado CIC de la EC-idCAT es de nivel 2 y se identifica 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 Administración Local (EC-AL)**

El certificado CIC de la EC-AL es de nivel 2 y se identifica 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 Universitats i Recerca (EC-UR)**

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

a) Certificado de Infraestructura de la Entidad de Certificación del Parlament de Catalunya (EC-Parlament)

El certificado CIC de la EC-Parlament es de nivel 2 y se identifica 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 SectorPúblic (EC-SECTORPUBLIC)**

El certificado CIC de la EC-SECTORPUBLIC es de nivel 2 y se identifica 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 Ciutadania (EC-CIUTADANIA)**

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

- Los CIC de nivel 3 se identifican con el identificador de objeto (OID): 1.3.6.1.4.1.15096.1.3.1.13.

  - **Certificado de Infraestructura de la Entidad de Certificación de Universitat Rovira i Virgili (EC-URV)**

El certificado CIC de la EC-URV es de nivel 3 y se identifica con el identificador de objeto (OID): 1.3.6.1.4.1.15096.1.3.1.13.

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

Los certificados CIPISR de clase 1 emitidos por la EC-ACC se 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-ACC 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-ACC se 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-ACC se 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-ACC se 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-ACC se 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-ACC se 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-ACC no se expiden al público, sino a:

- La propia 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 Administración Local (EC-AL).
- La Entidad de Certificación de la Universitat i Recerca (EC-UR).
- La Entidad de Certificación de la Universitat Rovira i Virgili (EC-URV).
- La Entidad de Certificación del Parlament de Catalunya (EC-Parlament).

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

Conforme a esta función,el Consorci AOC será responsable por la actuación de la EC-ACC 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

La Entidad de Certificación Raíz, que es el Consorci AOC, dispone de una autoridad de certificación principal, denominada “Raíz de la jerarquía pública de certificación de Catalunya” y tiene la finalidad de integrar otras entidades de certificación en el sistema público catalán de certifiación 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).

La huella digital del certificado de la Entidad de Certificación EC-ACC es:
28 90 3a 63 5b 52 80 fa e6 77 4c 0b 6d a7 d6 ba a6 4a f2 e8

1.3.3 Entidades de certificación vinculadas

Las Entidades de Certificación Vinculadas son las instituciones, a las que el prestador del servicio de certificación presta los servicios de expedición y gestión de los certificados mediante las autoridades de certificación, y que se encuentran inscritas en la jerarquía pública de certificación de Catalunya.

Con una Entidad de Certificación Vinculada, la institución emite certificados a otras entidades de certificación vinculadas o a usuarios finales, mediante la emisión de los certificados de infraestructura, personales, de entidad, de dispositivos y de objetos.

Cuando la institución delega en el Consorci AOC la operación de la entidad de certificación vinculada, en su calidad legal de prestador de servicios de certificación, la institución permanece responsable de la organización y las decisiones de gestión referidas a la entidad de certificación. Esta función, que no puede ser objeto de delegación, se llama Entidad de Certificación Virtual.

El Consorci AOC puede crear, a su vez, Entidades de Certificación Vinculadas de su propia titularidad, cuando no exista una institución única responsable de una comunidad de usuarios que precisen certificados.

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-ACC;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 de la Universitat i Recerca (EC-UR).
    - La Entidad de Certificación de la Universitat Rovira i Virgili (EC-URV).
    - 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-ACC 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 Raíz de la jerarquía (EC-ACC).
- La Entidad de Certificación de la Generalitat de Catalunya (EC-GENCAT).
- 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 de la Universitat Rovira i Virgili (EC-URV).
- 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. Certificados de infraestructura

1.4.1.1.1. 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 el Consorci AOC, 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, CIV, CPSR, CPSA, CPISR, CPISA, CPIXSA, CPI, CPX, CEISR, CEX, CDS, CDSCD, CDS-1 Sede electrónica, CDA, CDA-1 Sello electrónico, CDP y COS.
- Emisión y firma de listas de revocación de certificados (LRC).

a. Certificado de Infraestructura de Entidad de Certificación Raíz (CIC Raíz)

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).

b. Certificado de Infraestructura de la Entidad de Certificación de la Generalitat de Catalunya (EC-GENCAT)

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

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

c. Certificado de Infraestructura de la Entidad de Certificación SectorPúblic (EC-SECTORPUBLIC)

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

- Emisión y firma de certificados:CPISR-1, CPX-1, CPISR-1 Cargo Uso, CPISR-1 Cargo, CPX-1 Cargo, CPISR-2 Cargo, CPX-2 Cargo, CPPISR-1 Cargo, CPPISR-2 Cargo, CEISR-1, CEX-1, CIPISR-1, CIPISR-2, CDS-1, CDSCD-1, CDS-1 Sede Electrónica, CDP-1, CDA-1 y CDA-1 Sello electrónico, CIPISR-1, CIPISR-2.
- Emisión y firma de listas de revocación de certificados (LRC).

d. Certificado de Infraestructura de la Entidad de Certificación Ciutadania (EC-CIUTADANIA)

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

- Emisión y firma de certificados:CIPISR-1, CIPISR-2, CPIXSA-2.
- Emisión y firma de listas de revocación de certificados (LRC).

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

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

- Emisión y firma de certificados:CPISR-1, CPX-1, CPISR-1 Cargo Uso, CPISR-1 Cargo, CPX-1 Cargo, CPISR-2 Cargo, CPX-2 Cargo, CEISR-1, CEX-1, CIPISR-1, CIPISR-2, CDS-1, CDSCD-1, CDS-1 Sede Electrónica, CDP-1, CDA-1 y CDA-1 Sello electrónico, CIPISR-1, CIPISR-2.
- Emisión y firma de listas de revocación de certificados (LRC).

f. Certificado de Infraestructura de la Entidad de Certificación de Ciudadanos (EC-idCAT)

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

- Emisión y firma de certificados CPISA y CPIXSA.
- Emisión y firma de listas de revocación de certificados (LRC).

g. Certificado de Infraestructura de la Entidad de Certificación de la Administración Local (EC-AL)

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

- Emisión y firma de certificados CPISR-1, CPX-1, CPISR-1 Cargo Uso, CPISR-1 Cargo, CPX-1 Cargo, CPISR-2 Cargo, CPX-2 Cargo, CEISR-1, CEX-1, CIPISR-1, CIPISR-2, CDS-1, CDSCD-1, CDS-1 Sede Electrónica, CDP-1, CDA-1 y CDA-1 Sello electrónico, CIPISR-1, CIPISR-2.
- Emisión y firma de listas de revocación de certificados (LRC).

h. Certificado de Infraestructura de la Entidad de Certificación de Universitats i Recerca (EC-UR)

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

- Emisión y firma de certificados CPISR-1 Cargo, CPISR-1 Cargo Extranjero, CPX-1 Cargo, CPX-1 Cargo Extranjero, CPISR-2 Cargo, CPX-2 Cargo, CPISR-2 Estudiante, CPX-2 Estudiante, CPISR-2 Estudiante Extranjero, CPX-2 Estudiante Extranjero, CEISR-1, CEX-1, CDS-1, CDSCD-1, CDS-1 Sede electrónica, CDP-1, CDA-1, CDA-1 Sello electrónico, CIPISR-1 y CIPISR-2.
- Emisión y firma de listas de revocación de certificados (LRC).

i. Certificado de Infraestructura de la Entidad de Certificación de Universitat Rovira i Virgili (EC-URV)

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

- Emisión y firma de certificados CPISR-1 Cargo, CPISR-1 Cargo Extranjero, CPX-1 Cargo, CPX-1 Cargo Extranjero, CPISR-2 Cargo, CPX-2 Cargo, CPISR-2 Estudiante, CPX-2 Estudiante, CPISR-2 Estudiante Extranjero, CPX-2 Estudiante Extranjero, CEISR-1, CEX-1, CDS-1, CDSCD-1, CDS-1 Sede electrónica, CDP-1, CDA-1, CDA-1 Sello electrónico, CIPISR-1 y CIPISR-2.

- Emisión y firma de listas de revocación de certificados (LRC).

j. Certificado de Infraestructura de la Entidad de Certificación del Parlament de Catalunya (EC-Parlament)

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

- Emisión y firma de certificados CPISR-1 Cargo, CPX-1 Cargo,CPISR-2 Cargo, CPX-2 Cargo, CEISR-1, CEX-1, CDS-1, CDSCD-1, CDS-1 Seu electrónica, CDA-1, CDA-1 Segell electrònic, CDP-1, CIPISR-1 y CIPISR-2.

Emisión y firma de listas de revocación de certificados (LRC).

1.4.1.1.2. 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.

1.4.1.1.3. 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.

1.4.1.1.4. 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.

1.4.1.1.5. 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.

1.4.1.1.6. 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.

1.4.1.1.7. 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 CI

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 digitaldel 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-ACC 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-ACC, 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-ACC

La EC-ACC 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-ACC, 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-ACC 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-ACC, pudiendo ser consultadas por los interesados.

La información de estado de revocación de certificados se publica de acuerdo con lo establecido en la sección **Error! No s'ha trobat l'origen de la referència.***Frecuencia de emisión de listas de revocación de certificados (LRCs).*

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-ACC 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-ACC 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-ACC 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-ACC.

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-ACC 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-ACC denominado “Ceremonia de Claves”, descrito en la sección correspondiente de la presente DPC.

3.2.2.2 Entidades de Registro

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

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

3.2.4. Información no verificada

La entidad suscriptora del certificado 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

Tanto si se trata de una renovación rutinaria como si es posterior a la revocación del certificado a renovar, el proceso a seguirpara la renovación de un certificado será el mismo que para la emisión de certificados nuevos: la EC-ACC 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-ACC, 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-ACC 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-ACC 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-ACC, 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-ACC deniega la petición. En el supuesto de que las irregularidades no puedan corregirse, la EC-ACC deniega la solicitud definitivamente.

- Si la verificación es correcta, la EC-ACC:
  - 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-ACC 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-ACC durante el proceso de emisión

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

- 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-ACC.
- 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-ACC 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-ACC:

- 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 delConsorci 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-ACC, 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-ACC.

Una vez registrado el cambio de estado del certificado en el sistema de la EC-ACC, 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-ACC.

La EC-ACC 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-ACC.

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 Consorci 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 claves para los certificados de firma electrónica emitidos por la EC-ACC.

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

La EC-ACCse asegura de la aplicación de los procedimientos administrativos y de gestión, adecuados y conformes con los estándares reconocidos y, en particular:

a. Se realiza un análisis de gestión de riesgo para evaluar las necesarias medidas de seguridad.

b. Se es responsable por la provisión de los servicios de forma segura, incluso cuando una parte de los mismos sea subcontratada. Las responsabilidades de terceros son definidas y hay que implantar los necesarios controles jurídicos a fin de garantizar que los terceros cumplen con sus obligaciones con un nivel de seguridad equivalente.

c. Se establecen las normas principales en materia de seguridad mediante un órgano de alto nivel que define la política de seguridad de la información de la Entidad, y da la necesaria publicidad mediante acciones de comunicación interna.

d. Se mantiene en todo momento la infraestructura necesaria para gestionar la seguridad de las operaciones. Cualquier cambio que tenga impacto en el nivel de seguridad debe ser aprobado por el órgano referido en el número anterior.

e. Se documentan, implantan y mantienen los controles de seguridad y procedimientos de operación de las instalaciones, sistemas y activos de información en que se sustenta la prestación de los servicios.

f. En caso de subcontratación total de los servicios, se garantiza el mantenimiento del necesario nivel de seguridad de la información.

5.1 Controles de seguridad física

5.1.1 Áreas seguras

La EC-ACC dispone de instalaciones que protegen físicamente la prestación, al menos, de los servicios de generación de certificados, de dispositivos criptográficos y de gestión de revocación, del compromiso causado por acceso no autorizado a los sistemas o a los datos.

La protección física se consigue mediante la creación de perímetros de seguridad claramente definidos entorno a los servicios de generación de certificados, de dispositivos criptográficos y de gestión de revocación. La parte de las instalaciones compartida con otras organizaciones se encuentra fuera de estos perímetros.

5.1.2 Controles de seguridad física

La EC-ACC establece controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentran los sistemas, los mismos sistemas y los equipamientos utilizados para las operaciones. La política de seguridad física y ambiental aplicable a los servicios de generación de certificados, de dispositivos criptográficos y de gestión de revocación establece prescripciones para las siguientes contingencias:

- Controles de acceso físico.

- Protección ante desastres naturales.
- Medidas de protección ante incendios.
- Fallo de los sistemas de soporte (energía eléctrica, telecomunicaciones, etc.).
- Derribo de la estructura.
- Inundaciones.
- Protección antirrobos.
- Conformidad y entrada no autorizada.
- Recuperación del desastre.
- Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes utilizados para los servicios de la EC-ACC.

5.1.3 Localización y construcción de las instalaciones

La localización de las instalaciones permite la presencia de fuerzas de seguridad en un plazo de tiempo razonablemente inmediato desde que una incidencia les sea notificada.

La calidad y solidez de los materiales de construcción de las instalaciones garantiza unos adecuados niveles de protección ante intrusiones por fuerza bruta.

5.1.4 Acceso físico

La EC-ACC establece niveles de seguridad con restricción de acceso a los diferentes perímetros y barreras físicas definidas.

Para el acceso a las dependencias de la EC-ACC donde se lleven a cabo procesos relacionados con el ciclo de vida del certificado, es necesaria la autorización previa, identificación en el momento del acceso y registro del mismo, incluyendo filmación por circuito cerrado de televisión y su archivo.

Esta identificación, ante el sistema de control de accesos, se realiza mediante reconocimiento de algún parámetro biométrico del individuo, excepto en caso de visitas escoltadas.

La generación de claves criptográficas de la EC-ACC, así como su almacenaje, se realiza en dependencias específicas para estas finalidades, y requieren de acceso y permanencia dobles.

5.1.5 Electricidad y aire acondicionado

Los equipos informáticos de la EC-ACC están convenientemente protegidos ante fluctuaciones o cortes de subministro eléctrico, que puedan dañarlos o interrumpir el servicio.

Las instalaciones cuentan con un sistema de estabilización de la corriente, así como de un sistema de generación propio con autonomía suficiente para mantener el subministro durante el tiempo que requiera el cierre ordenado y completo de todos los sistemas informáticos.

Los equipos informáticos están ubicados en un entorno donde se garantice una climatización (temperatura y humedad) adecuada a sus condiciones óptimas de trabajo.

5.1.6 Exposición al agua

La EC-ACC dispone de sistemas de detección de inundaciones adecuados para proteger los equipos y activos ante tal eventualidad, en el caso que las condiciones de ubicación de las instalaciones lo hicieran necesario.

5.1.7 Advertencia y protección de incendios

Todas las instalaciones y activos de la EC-ACC cuentan con sistemas automáticos de detección y extinción de incendios.

En concreto, los dispositivos criptográficos, y soportes que almacenen claves de las Entidades de Certificación, tendrán que contar con un sistema específico y adicional al resto de la instalación, para la protección ante el fuego.

5.1.8 Almacenaje de soportes

El almacenaje en soportes de información se realiza de forma que se garantice tanto su integridad como su confidencialidad, de acuerdo con la clasificación de la información que se haya establecido.

Las copias se guardan en formato CD, y éstos en caja fuerte en la misma sala.

El acceso a estos soportes, incluso para su eliminación, está restringido a personas específicamente autorizadas.

5.1.9 Tratamiento de residuos

La eliminación de soportes, tanto papel como magnéticos, se realiza mediante mecanismos que garanticen la imposibilidad de recuperación de la información.

En el caso de soportes magnéticos, se procede al formateo, borrado permanente, o destrucción física del soporte.

En el caso de documentación en papel, éste se somete a un tratamiento físico de destrucción.

5.1.10 Copia de seguridad fuera de las instalaciones

Periódicamente, la EC-ACC almacena una copia de seguridad de los sistemas de información, en dependencias físicamente separadas de aquellas en las que se encuentran los equipos.

Se realizará una copia de seguridad incremental diaria y una copia de seguridad semanal.

En el momento de realizar una salida de información de las dependencias, se deben adoptar medidas adecuadas para impedir cualquier recuperación indebida de la mencionada información (como por ejemplo la utilización de carteras con dispositivos seguros de claves o combinaciones o la utilización de ficheros cifrados).

5.2 Controles de procedimientos

La EC-ACC 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-ACC realiza los procedimientos administrativos y de gestión de acuerdo con la política de seguridad de la EC-ACC.

5.2.1 Funciones fiables

Las personas que tengan que ocupar estos sitios son formalmente nominados por la alta dirección de la EC-ACC.

Las funciones fiables incluyen:

- Personal responsable de la seguridad
- Administradores del sistema
- Operadores del sistema
- Auditores del sistema
- Cualquier otra persona con acceso a datos de carácter personal

Las funciones y obligaciones fiables se definen en la sección 5.3 este documento.

5.2.2 Número de personas por tarea

Las funciones fiables identificadas en la política de seguridad de la EC-ACC, y sus responsabilidades asociadas, están documentadas en descripciones de lugares de trabajo.

5.2.3 Identificación y autenticación para cada función

La EC-ACC identifica y autentica el personal antes de acceder a la correspondiente función fiable.

5.2.4 Roles que requieren separación de tareas

La EC-ACC identifica, en su política de seguridad, funciones o roles fiables.

Las funciones fiables incluyen:

a. Oficial de Seguridad
b. Operador de registro
c. Administradores del sistema
d. Operadores del sistema
e. Auditores del sistema
f. Cualquier otra persona con acceso a datos de carácter personal

Las citadas restricciones se aplican en todo caso:

1. La persona que actúa como oficial de seguridad o como operador de registro no puede ser auditor del sistema.
2. La persona que actúa como administrador del sistema no puede ser oficial de seguridad ni auditor del sistema.

Las funciones y obligaciones fiables se definen en la sección 5.3 este documento.

5.3 Controles de personal

La EC-ACC 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-ACC.
- 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 la EC-ACC.

El Consori AOC, además, se ve afectado por el siguiente personal:

- 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

La EC-ACC ocupa personal cualificado y con la experiencia necesaria para la prestación de los servicios ofrecidos, en el ámbito de la firma electrónica y los procedimientos de seguridad y de gestión adecuada.

Este requisito se aplicará al personal de gestión de la EC-ACC, especialmente en relación con procedimientos de personal de seguridad.

La calificación y la experiencia pueden suplirse mediante una formación y entrenamiento apropiados.

El personal en sitios fiables se encuentra libre de intereses personales que entre en conflicto con el desarrollo de la función que tenga encomendada.

5.3.2 Requisitos de formación

La EC-ACC forma el personal en lugares fiables y de gestión, hasta que logran la calificación necesaria.

La formación incluye los siguientes contenidos:

- Principios y mecanismos de seguridad de la jerarquía pública de certificación de Catalunya, así como el entorno de usuario de la persona a formar.
- Versiones de maquinaria y aplicaciones en uso.
- Tareas que tiene que realizar la persona.
- Gestión y tramitación de incidentes y compromisos de seguridad.
- Procedimientos de continuidad de negocio y emergencia.
- Procedimiento de gestión y de seguridad en relación con el tratamiento de los datos de carácter personal.

La EC-ACC, además, proporciona a todo el personal involucrado en sus operaciones como Entidad de Registro, una información adecuada, que incluye los procedimientos de trabajo y los de seguridad. También se realiza instrucción periódica en normas de seguridad, planes de contingencia y gestión de incidencias.

5.3.3 Requisitos y frecuencia de actualización formativa

Todo el personal vinculado a la Entidad de Registro tiene como requisito imprescindible la asistencia al curso de formación de Entidades de Registro impartido por el Consori AOC.

5.3.4 Secuencia y frecuencia de rotación laboral

Sin estipulación adicional.

5.3.5 Sanciones por acciones no autorizadas

La EC-ACC dispone de un sistema sancionador, para depurar las responsabilidades derivadas de acciones no autorizadas.

Las acciones disciplinarias incluyen la suspensión y el despido de la persona responsable de la acción dañosa.

5.3.6 Requisitos de contratación de profesionales

La EC-ACC contrata profesionales para cualquier función, incluso para un lugar fiable, caso en el que se somete a los mismos controles que los empleados restantes.

En el caso que el profesional no tenga que someterse a estos controles, está constantemente acompañado por un empleado fiable.

En el caso que todos o una parte de los servicios de certificación sean operados por un tercero, los controles y previsiones realizadas en esta sección 5, o en otras partes de la política de certificado o de esta DPC, serán aplicados y completados por el tercero que realiza las funciones de operación de los servicios de certificación. La EC-ACC es responsable, en todo caso, de la efectiva ejecución.

Estos aspectos quedan concretados en el instrumento jurídico utilizado para acordar la prestación de los servicios de certificación por el tercero diferente a la EC-ACC.

5.3.7 Suministro de documentación al personal

La EC-ACC suministra la documentación que estrictamente necesite su personal en cada momento, con el fin que sea suficientemente competente.

5.4 Procedimientos de auditoría de seguridad

5.4.1 Tipos de acontecimientos registrados

La EC-ACC guarda registro, como mínimo, de los siguientes acontecimientos relacionados con la seguridad de la entidad:

- El encendido y apagado de los sistemas.
- El inicio y la finalización de la aplicación de Autoridad (técnica) de certificación.
- Los intentos de crear, borrar, cambiar contraseñas o permisos de los usuarios dentro del sistema.
- Los cambios en las claves de la Autoridad (técnica) de certificado.

- Los cambios en las políticas de emisión de certificados.
- Los intentos de entrada y salida del sistema.
- Los intentos no autorizados de entrada en la red de la EC-ACC.
- Los intentos no autorizados de acceso a los ficheros del sistema.
- La generación de las claves de la EC-ACC.
- Los intentos nulos de lectura y escritura en un certificado y en el Depósito.
- Acontecimientos relacionados con el ciclo de vida del certificado, como una solicitud, emisión, revocación y renovación de un certificado.
- Acontecimientos relacionados con el ciclo de vida del módulo criptográfico, como recepción, uso y desinstalación de éste.

La EC-ACC también guarda, ya sea manual o electrónicamente, la siguiente información:

- La ceremonia de generación de claves y las bases de datos de gestión de claves.
- Registros de acceso físico.
- Mantenimientos y cambios de configuración del sistema.
- Cambios en el personal.
- Informes de compromisos y discrepancias.
- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal del suscriptor.
- Posesión de datos de activación, para operaciones con la clave privada de la EC-ACC.
- Informes completos de los intentos de intrusión física en las infraestructuras que dan soporte a la emisión y gestión de certificados.

5.4.2 Frecuencia de tratamiento de registros de auditoría

Los registros de auditoría se examinan al menos una vez a la semana en búsqueda de actividad sospechosa o no habitual.

El procesamiento de los registros de auditoría consiste en una revisión de los registros que incluye la verificación que estos no han sido manipulados, una breve inspección de todas las entradas de registro y una investigación más profunda de cualquier alerta o irregularidad en los registros. Las acciones realizadas a partir de la revisión de auditoría también se encontrarán documentadas.

5.4.3 Periodo de conservación de registros de auditoría

Los registros de auditoría se retienen durante al menos dos meses después de procesarlos y a partir de ese momento se archivan de acuerdo con la sección 5.5 de la presente DPC.

5.4.4 Protección de los registros de auditoría

Los ficheros de registros, tanto manuales como electrónicos, se protegen de lecturas, modificaciones, borrados o cualquier otro tipo de manipulación no autorizada usando controles de acceso lógico y físico.

5.4.5 Procedimientos de generación de copias de seguridad

Se generan copias de soporte incrementales de registro de auditoría diariamente y copias completas semanalmente.

Con el fin de conservar correctamente las copias de seguridad se han implantado los siguientes puntos:

- Se guardan en armarios ignífugos.
- Solamente personas autorizadas disponen de acceso a las copias de seguridad.
- Las copias están identificadas.
- Si un material ha contenido a copias de seguridad (disquetes, DVD's...) y se quieren reutilizar se asegura que los datos que ha contenido sean totalmente borrados haciendo imposible su recuperación.
- Se autoriza expresamente la extracción de las copias de seguridad fuera de la Entidad de Registro, rellenando una ficha al respecto y anotando el correspondiente detalle en un libro de registro.
- Se procura ir depositando copias de seguridad periódicamente fuera de la Entidad de Registro.

5.4.6 Localización del sistema de acumulación de registros de auditoría

El sistema de acumulación de registros de auditoría es, al menos, un sistema interno de la EC-ACC, compuesto por los registros de la aplicación, por los registros de red y por los registros del sistema operativo, además de por los datos manualmente generados, que serán almacenados por el personal debidamente autorizado.

5.4.7 Notificación del acontecimiento de auditoría al causante del acontecimiento

Cuando el sistema de acumulación de registros de auditoría registra un acontecimiento, no es necesario enviar una notificación al individuo, organización, dispositivo o aplicación que causó el acontecimiento.

Se comunica si el resultado de su acción ha tenido éxito o no, pero no que se ha auditado la acción.

5.4.8 Análisis de vulnerabilidades

Los acontecimientos en el proceso de auditoría son guardados, en parte, para monitorizar las vulnerabilidades del sistema.

Los análisis de vulnerabilidad son ejecutados, repasados y revisados por medio de un examen de estos acontecimientos monitorizados

Estos análisis son ejecutados diariamente, mensualmente y anualmente de acuerdo con su definición en el Plan de Auditoría de la EC-ACC.

5.5 Archivo de informaciones

La EC-ACC garantiza que toda la información relativa a los certificados se guarda durante un periodo de tiempo apropiado, según lo establecido en la sección 5.5.2 d'aquesta DPC.

5.5.1 Tipos de acontecimientos registrados

La EC-ACC guarda todos los acontecimientos que tengan lugar durante el ciclo de vida de un certificado, incluyendo la renovación de éste.

La EC-ACC guarda un registro de lo siguiente:

Documentos originales:

- Formulario de solicitud de certificados.
- Certificado de datos.
- Hoja de entrega de suscriptor de certificados.

5.5.2 Periodo de conservación de registros

5.5.2.1 Requisitos para todos los tipos de certificados

La EC-ACC guarda los registros especificados en la sección 5.5.1 de la presente DPC durante 5 años, contados desde el momento de la expedición del certificado. Tota la informació relativa als Certificats d'Infraestructura de Certificació es guarda de forma permanent.

5.5.2.2 Requisitos específicos para los certificados CIPISR

No obstante lo dispuesto en la sección 5.2.2.1 anterior, la EC-ACC guarda los registros de los certificados CIPISR durante 15 años, contados desde el momento de la expedición de los mismos.

5.5.3 Protección del archivo

La EC-ACC:

- Mantiene la integridad y la confidencialidad del archivo que contiene los datos referentes a los certificados emitidos.
- Archiva los datos indicados anteriormente de forma completa y confidencial.
- Mantiene la privacidad de los datos de registro del suscriptor.

5.5.4 Procedimientos de generación de copias de seguridad

Un técnico de comunicaciones de la EC-ACC se encarga de hacer y verificar la realización de las copias de seguridad de los logs de acceso lógico al sistema operativo de la LRA.

Estas copias de seguridad se realizan con una periodicidad mensual y se guardan en formato CD, y estos discos en una caja fuerte presente en la misma sala.

Se realizan también copias de seguridad de la aplicación KeyOne personalizada para la EC-ACC. Estas copias las guarda el Consori AOC en sus instalaciones.

5.5.5 Requisitos de sellado de cautela de fecha y hora

La EC-ACC emite los certificados y las LRC con información de tiempo y hora.

5.5.6 Localización del sistema de archivo

La EC-ACC tiene un sistema de mantenimiento de datos de archivo fuera de sus propias instalaciones, así como se especifica en la sección 5.1.10 de la presente DPC.

5.5.7 Procedimientos de obtención y verificación de información de archivo

Sólo las personas autorizadas por la EC-ACC tienen acceso a los datos de archivo, ya se encuentren éstos en las mismas instalaciones de la EC-ACC o en su ubicación externa.

5.6 Renovación de claves

Los certificados de la EC-ACC que se hayan renovado, se comunican a los usuarios finales, mediante su publicación en el directorio del Consorci AOC.

5.7 Compromiso de claves y recuperación de desastre

5.7.1 Procedimiento de gestión de incidencias y compromisos

La EC-ACC 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-ACC 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-ACC (o plan de recuperación de desastres) considera el compromiso o la sospecha de compromiso de la clave privada de la EC-ACC como un desastre.

En caso de compromiso la EC-ACC:

- 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-ACC ya no son válidos.

5.7.4 Desastre sobre las instalaciones

La EC-ACC 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-ACC 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-ACC 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-ACC tienen las medidas de seguridad físicas especificadas en el Plan de Seguridad.

5.8 Finalización del servicio

5.8.1 EC-ACC

La EC-ACC asegura que las posibles interrupciones a los suscriptores y a terceras partes son mínimas como consecuencia del cese de los servicios de la EC-ACC y, en particular, asegura un mantenimiento continuo de los registros requeridos para proporcionar evidencia de certificación en procedimientos legales.

Antes de acabar sus servicios la EC-ACC ejecuta, como mínimo, los siguientes procedimientos:

- Informa a todos los suscriptores y verificadores (no se requiere que la EC-ACC tenga alguna relación anterior con terceras partes).
- Termina toda autorización de subcontrataciones que actúen en nombre de la EC-ACC en el proceso de emisión de certificados.
- Ejecuta las tareas necesarias para transferir las obligaciones de mantenimiento de la información de registro y los archivos de registro de acontecimientos durante los periodos de tiempo respectivos indicados al suscriptor y a los verificadores.
- Destruye las claves privadas de la EC-ACC o las retira del uso.

La EC-ACC declara en sus prácticas las previsiones que tiene que adoptar para el caso de finalización del servicio. Éstas incluyen:

- Notificación a las entidades afectadascon una antelación mínima de 2 meses a la finalización efectiva del servicio.
- Transferencia de las obligaciones de la EC-ACC a otras personas, bajo su consentimiento.
- Cómo se trata el estado de revocación de los certificados emitidos que aún no han expirado.

La EC-ACC transfiere los certificados, en los términos previstos en la Ley 59/2003, de 19 de diciembre, de firma electrónica.

5.8.2 Entidad de Registro

Sin estipulación adicional.

6. Controles de seguridad técnica

La EC-ACC 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-ACC.

6.1.2 Envío de la clave privada al suscriptor

La clave privada del suscriptor, le es entregada debidamente protegida mediante una tarjeta inteligente que cumple los requisitos establecidos por las especificaciones técnicas CEN CWA 14169 y CWA 14170 o equivalente.

6.1.3 Envío de la clave pública al emisor del certificado

El método de envío de la clave pública a la EC-ACC es PKCS #10, otra prueba criptográfica equivalente o cualquier otro método aprobado por el Consorci AOC.

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

La clave de la EC-ACC 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-ACC, en forma de certificado auto firmado, junto a una declaración referente a que la clave permite autenticar a la EC-ACC.

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-ACC se publica en el Directorio de la EC-ACC, en forma de certificado CIC firmado por el Consorci AOC.

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

Adicionalmente, en aplicaciones S/MIME, el mensaje de datos contiene una cadena de certificados, incluyendo certificados CIC con las claves públicas de las Entidades de Certificación de la jerarquía, que de esta forma son distribuidas a los usuarios.

6.1.5 Medidas de claves

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

Las claves de todos los certificados emitidos por la EC-ACC 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

Se realiza de acuerdo con la especificación técnica ETSI TS 102 176, que indica la calidad de los algoritmos de firma electrónica.

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

Los pares de claves de la EC-ACC son generados utilizando hardware criptográfico que cumple los requisitos establecidos por la especificación técnica CEN CWA 141617 o equivalente.

Los pares de claves de los suscriptores de certificados CIPISR deben generarse en tarjetas inteligentes o en dispositivos criptográficos que cumplen los requisitos establecidos por las especificaciones técnicas CEN CWA 14169 y CWA 14170 o equivalente.

La generación de claves para el resto de certificados puede realizarse mediante aplicaciones informáticas.

6.1.9 Propósitos de uso de claves

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

La extensión Key Usage se utilizará para establecer límites técnicos a los usos que se pueda dar a una clave privada correspondiente a una clave pública listada en un certificado X.509v3. Debe tenerse en cuenta que la efectividad de las limitaciones basadas en extensiones de certificados depende en ocasiones de la operación de aplicaciones informáticas que no han sido fabricadas ni pueden ser controladas por el Consorci AOC.

6.2 Protección de la clave privada

6.2.1 Estándares de módulos criptográficos

6.2.1.1.Estándares de los módulos criptográficos

Las claves privadas de las Entidades de Certificación se protegen utilizando hardware criptográfico que cumple los requisitos establecidos por la especificación técnica FIPS 140-2 Nivel 3 o superior.

Los pares de claves de los suscriptores de certificados de firma reconocida y de certificados de nivel alto están protegidos por tarjetas inteligentes que cumplen los requisitos establecidos por la especificación técnica CEN CWA 14169 o equivalente.

6.2.1.2.Ciclo de vida de las tarjetas con circuito integrado

Las tarjetas con circuito integrado (también tarjetas inteligentes) se entregan en cada emisión de nuevo certificado por la Entidad de Registro.

Por cada nueva emisión o renovación de los certificados se entrega una tarjeta nueva, es decir, no se carga certificados en tarjetas usadas.

Cuando el Consorci AOC detecte errores o defectos en las tarjetas, podrá retirar de oficio las tarjetas afectadas. En caso de detectar defectos o errores en casos puntuales, se sustituirá la tarjeta afectada, previa revocación del certificado y se emitirá un nuevo certificado que se librará en una tarjeta nueva sin coste adicional para el suscriptor.

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

De los 5 posibles dispositivos criptográficos que existen, la EC-ACC requiere la concurrencia de al menos 2 de forma simultánea.

Cada uno de estos dispositivos es responsabilidad de una persona concreta, única conocedora de la clave de acceso al mismo. La clave de acceso es conocida únicamente por una persona responsable de este dispositivo. Ninguna de ellas conoce más que una de las claves de acceso.

Los dispositivos criptográficos quedan almacenados en las dependencias de la EC-ACC, y para su acceso es necesaria una persona adicional.

6.2.3 Depósito de la clave privada

Las claves privadas de la EC-ACC se almacenan en espacios ignífugos y protegidos por controles de acceso físico doble.

6.2.4 Copia de seguridad de la clave privada

Existe copia de seguridad de la clave privada de la EC-ACC y de los medios necesarios para acceder, en dependencia independiente de aquella donde se almacena habitualmente.

6.2.5 Archivo de la clave privada

La clave privada de la EC-ACC cuenta con una copia de seguridad realizada, almacenada, y recuperada en su caso por personal sujeto a la política de confianza del personal. Este personal está expresamente autorizado para estas finalidades, y se limita a aquel que necesite hacerlo en las prácticas de la EC-ACC.

Los controles de seguridad a aplicar en copias de seguridad de la EC-ACC son de igual o superior nivel a las que se apliquen a las claves habitualmente en uso.

Cuando las claves se almacenen en un módulo hardware de proceso dedicado, se proveen los controles oportunos para que estas nunca puedan abandonar el dispositivo.

6.2.6 Introducción de la clave privada en el módulo criptográfico

Las claves privadas de la EC-ACC quedan almacenadas en ficheros cifrados con claves fragmentadas y en tarjetas inteligentes (de las que no pueden ser extraídas).

Estas tarjetas son utilizadas para introducir la clave privada en el módulo criptográfico.

6.2.7 Almacenaje de la clave privada en el módulo criptográfico

Las claves privadas se generan directamente en los módulos criptográficos.

6.2.8 Método de activación de la clave privada.

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

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

Para certificados CIPISR, cuando la tarjeta inteligente o dispositivo criptográfico se retire del dispositivo lector, será necesaria nuevamente la introducción del PIN.

6.2.10 Método de destrucción de la clave privada

Las claves privadas son destruidas de forma que impida su robo, modificación, divulgación o uso no autorizado.

6.2.11 Clasificación de los módulos criptográficos

Los módulos de la EC-ACC obtienen o superan el nivel EAL 4 de Common Criteria (ISO 15408) con los aumentos que se determinen en la especificación técnica CEN CWA 14167.

Los módulos de los suscriptores de certificados CIPISR obtienen o superan el nivel EAL 4 de Common Criteria (ISO 15408) con los aumentos que se determinan en la especificación técnica CEN CWA 14169.

6.3 Otros aspectos de gestión del par de claves

6.3.1 Archivo de la clave pública

La EC-ACC 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

Los periodos de utilización de las claves son los determinados por la duración del certificado, y una vez transcurrido no se pueden continuar utilizando.

Como excepción, la clave privada de descifrado puede continuar utilizándose hasta después de la expiración del certificado.

6.4 Datos de activación

6.4.1 Generación e instalación de los datos de activación

La EC-ACC facilita al suscriptor, por un lado los datos de activación de la tarjeta, y al cabo de 3 días la tarjeta.

6.4.2 Protección de datos de activación

6.4.2.1 Para certificados CIPISR

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 Entidad de Registro hace entrega al poseedor de claves el siguiente material:
  - Hoja de entrega de poseedor
  - Tarjeta con los certificados
  - Software necesario para utilizar la tarjeta
  - Carta de entrega de certificados.
- Al mismo tiempo, y por correo electrónico, se envían al poseedor de claves los datos de activación del certificado

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

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

Se garantiza que el acceso a los sistemas está limitado a individuos debidamente autorizados. En particular:

- La EC-ACC garantiza una administración efectiva del nivel de acceso de los usuarios (operadores, administradores, así como de cualquier usuario con acceso directo al sistema) para mantener la seguridad del sistema, incluyendo la gestión de cuentas de usuario, auditoría y modificaciones o denegaciones de acceso oportunas.
- La EC-ACC garantiza que el acceso a los sistemas de información y aplicaciones se restringe de acuerdo a lo establecido en la política de control de acceso, así como que los sistemas proporcionan los controles de seguridad suficientes para implementar la segregación de funciones identificada en las prácticas de la EC-ACC, incluyendo la separación de funciones de administración de los sistemas de seguridad y de los operadores. En concreto, el uso de programas de utilidades del sistema está restringido y estrechamente controlado.
- El personal de la EC-ACC está identificado y reconocido antes de utilizar aplicaciones críticas relacionadas con el ciclo de vida del certificado.
- El personal de la EC-ACC es responsable y tiene que poder justificar sus actividades, por ejemplo mediante un archivo de acontecimientos.
- Debe evitarse la posibilidad de revelación de datos sensibles mediante la reutilización de objetos de almacenaje (por ejemplo ficheros borrados) que queden accesibles a usuarios no autorizados.
- Los sistemas de seguridad y monitorización permiten una rápida detección, registro y actuación ante intentos de acceso irregulares o no autorizados a sus recursos (por ejemplo, mediante un sistema de detección de intrusiones, monitorización y alarma).
- El acceso a los depósitos públicos de la información de la EC-ACC (por ejemplo, certificados o información de estado de revocación) cuenta con un control de accesos para modificaciones o borrado de datos.

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

Se realiza un análisis de requisitos de seguridad durante las fases de diseño y especificación de requisitos de cualquier componente utilizada en las aplicaciones de

Autoridad (técnica) de certificación y de Autoridad (técnica) de Registro, para garantizar que los sistemas son seguros.

Se utilizan procedimientos de control de cambios para las nuevas versiones, actualizaciones y parches de emergencia, de dichos componentes.

6.6.2 Controles de gestión de seguridad

La EC-ACC garantiza que sus funciones de gestión de las operaciones de los módulos criptográficos son suficientemente seguras y, en particular, debe asegurar que existen instrucciones para:

a. Operar los módulos de forma correcta y segura.

b. Instalar los módulos minimizando el riesgo de fallo de los sistemas.

c. Proteger los módulos contra virus y software malicioso, para garantizar la integridad y validez de la información que procesan.

La EC-ACC mantiene un inventario de todos los activos informáticos y realiza una clasificación de los mismos de acuerdo con sus necesidades de protección, coherente con el análisis de riesgos efectuado.

La configuración de los sistemas se audita de forma periódica, de acuerdo con lo establecido en la sección 8.1.

Se realiza un seguimiento de las necesidades de capacidad, y se planificarán procedimientos para garantizar suficiente disponibilidad electrónica y de almacenaje para los activos informáticos.

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-ACC 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-ACC.
- 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

Esta sección se encuentra en la web (**http://www.aoc.cat/catcert**).

7.2 Perfil de la lista de revocación de certificados

Esta sección se encuentra en la web (**http://www.aoc.cat/catcert**).

8. Auditoría de conformidad

La EC-ACC 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.

A parte de la auditoria de conformidad, la EC-ACC realiza otras revisiones de carácter puntual para demostrar su confianza. Así, cuando se acepta una nueva Entidad de Certificación subordinada a la jerarquía, se realiza una revisión de los documentos de seguridad, DPC y PdC del Consorci AOC para asegurar que cumple con los requisitos de seguridad i de operación necesarios para formar parte de la Jerarquía de Entidades de Certificación del Consorci AOC.

Asimismo, si se sospecha que una Entidad de Certificación en funcionamiento no cumple alguno de los requisitos de seguridad o si se ha detectado un compromiso de claves, o cualquier acontecimiento que pueda suponer un peligro para la seguridad o integridad de la Entidad de Certificación Vinculada, se llevará a cabo una auditoría interna.

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

8.1 Frecuencia de la auditoría de conformidad

La EC-ACC lleva a término una auditoría de conformidad anualmente, además de las auditorías internas que realiza bajo su propio criterio o en cualquier momento, a causa de una sospecha de incumplimiento de alguna medida de seguridad o por un compromiso de claves.

8.2 Identificación y calificación del auditor

El Consorci AOC puede encargarse, mediante personal interno, de realizar la auditoría de conformidad.

No obstante la EC-ACC puede acudir a un auditor independiente 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-ACC auditada. En caso de auditoría interna la EC-ACC se ha de asegurar de que no existe conflicto de intereses que afecte negativamente su capacidad de realizar servicios de auditoría.

8.4 Relación de elementos objeto de auditoría

Los elementos objeto de auditoría serán los siguientes:

- Procesos de Autoridades de Certificación y elementos relacionados.
- Sistemas de información.
- Protección del centro de proceso.
- Documentación.

8.5 Acciones a emprender como resultado de una falta de conformidad

Una vez recibido el informe de la auditoría de cumplimiento llevada a término, la EC-ACC discute, con la entidad que ha ejecutado la auditoría y con el Consorci AOC, las deficiencias encontradas y desarrolla y ejecuta un plan correctivo que soluciona dichas deficiencias.

Si la EC-ACC auditada es incapaz de desarrollar y/o ejecutar dicho plan o si las deficiencias encontradas suponen una amenaza inmediata para la seguridad o integridad del sistema tiene que realizarse una de las siguientes acciones:

- Revocar la clave de la EC-ACC, de la forma como se describe en la sección 4.9.
- Acabar el servicio de la EC-ACC, de la forma como se describe en la sección 5.8.

8.6 Tratamiento de los informes de auditoría

La EC-ACC entrega los informes de resultados de auditoría al Consorci AOC en calidad de Entidad de Certificación Raíz de la jerarquía pública de certificación de Catalunya, en un plazo máximo de 15 días después de la ejecución de la auditoría.

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-ACC, en la prestación de sus servicios. Las tarifas se pueden consultar en la web delConsorci AOC (http://www.aoc.cat/catcert/).

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 AOC no 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 AOC dispone 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 delConsorci AOC como prestador de servicios de certificación.

En caso de uso incorrecto o no autorizado de los certificados, El Consorci AOC (o la EC correspondiente) no actuará como agente fiduciario frente a suscriptores y terceras personas, que deberán dirigirse contra el infractor de las condiciones de uso de los certificados establecidas por El Consorci AOC (o la EC correspondiente).

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

Las siguientes informaciones son mantenidas de forma confidencial por la EC-ACC:

a. Información de negocio suministrada por sus proveedores y otras personas con las que El Consorci AOC o la EC-ACC tiene una obligación de guardar secreto, establecida legal o convencionalmente.
b. Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.
c. Registros de auditoría interna y externa, creados y/o mantenidos por la EC-ACC y sus auditores.
d. Planes de continuidad de negocio y de emergencia.
e. Política y planes de seguridad.
f. Documentación de operaciones y resto de planes de operación, tal como el archivo, monitorización y otros análogos.
g. Cualquier otra información identificada como “Confidencial”.

9.3.2 Informaciones no confidenciales

Las siguientes informaciones no tienen carácter confidencial:

a. Esta Declaración de Prácticas de Certificación de la EC-ACC.
b. Cualquier otra información identificada como “Pública”.

9.3.3 Responsabilidad para la protección de información confidencial

La EC-ACC es responsable del establecimiento de las medidas apropiadas de protección de la información confidencial.

Estas medidas incluyen las cláusulas apropiadas de información confidenciales en los instrumentos jurídicos con todas las personas.

9.4 Protección de datos personales

9.4.1 Política de Protección de Datos Personales

El Consorci AOC desarrolla una política de protección de datos personales, de acuerdo con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y la normativa reglamentaria de aplicación en materia de protección de datos de carácter personal.

Con motivo de la prestación de servicios propios de certificación digital, resulta responsable de los ficheros "suscriptores de certificados" y "Personas físicas certificadas", creados de conformidad con la LOPD y notificados al Registro de la Agencia Catalana de Protección de Datos.

La estructura de los ficheros de datos de carácter personal es la siguiente:

SUSCRIPTORES DE CERTIFICADOS:

- Datos identificativos del colectivo suscriptor: nombre de la entidad o del organismo que solicita los certificados, CIF, dirección postal completa, dirección electrónica, página web.
- Datos identificativos de la persona que asume el rol de responsable del servicio: nombre, apellidos, DNI o equivalente, teléfono, fax, dirección postal, dirección electrónica.

PERSONAS FÍSICAS CERTIFICADAS:

- Datos identificativos: nombre, apellidos y DNI o equivalente de la persona física certificada. Opcionalmente, otros datos personales cuya inclusión sea solicitada para la persona autorizada, como el código CIP de la Tarjeta Individual Sanitaria.
- Datos de contacto: dirección postal completa a efectos de notificaciones, así como la dirección electrónica.
- Datos de la entidad a la que prestan sus servicios (sólo en caso de certificados de clase 1 y clase 2 de colectivo).
- Denominación de la entidad CIF, área de adscripción política, orgánica, laboral o profesional.

Los datos recogidos y tratados por el prestador de servicios de certificación tienen la consideración legal de datos de nivel básico.

El Consorci AOC desarrolla procedimientos indicados en este documento, que aplica en la prestación de sus servicios, en los cuales, en cumplimiento de los requisitos establecidos por las políticas de certificados que gestiona, y de acuerdo con el artículo 19 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, se detallan los requisitos y obligaciones en relación con la obtención y gestión de los datos personales que obtenga, cumpliendo a este efecto, las disposiciones de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal (RLOPD).

El Consorci AOC establece las medidas de seguridad de carácter técnico y organizativo necesarias para dar cumplimiento a las medidas de seguridad aplicables a ficheros automatizados del RLOPD. Con carácter meramente informativo se detallan a continuación las medidas aplicadas, el precepto del RLOPD y la sección de este documento y de la Política General de Certificación delConsorci AOC donde se desarrollan:

a. Ámbito de aplicación del documento de seguridad con especificación detallada de los recursos protegidos (artículo 88 del RD 1720/2007) – sección 6.1.

b. Medidas, normas, procedimientos, regla y estándares que garantizan el nivel de seguridad exigido por el RD 1720/2007 –sección 6.1 y, en general, todos los controles técnicos de las secciones 5 y 6 de la Política General de Certificación delConsorci AOC.

c. Funciones y obligaciones del personal (artículo 89 del RD 1720/2007) – sección 5.3.

d. Registro de incidencias (artículo 90 del RD 1720/2007), procedimiento de notificación, gestión y respuesta ante las incidencias - sección 9.4.5.

e. Control de acceso (artículo 91 del RD 1720/2007) – secciones 5 i 6.

f. Gestión de soportes (artículo 92 del RD 1720/2007) – sección 5.

g. Identificación i autenticación (artículo 93 del RD 1720/2007) – sección 5.2.

h. Procedimientos de copia de seguridad i recuperación de datos (artículo 94 del RD 1720/2007) - sección 5.5.

9.4.2 Datos de carácter personal no disponibles a terceros

De conformidad con lo establecido en el artículo 3 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal se consideran datos de carácter personal, se consideran datos de carácter personal cualquier información relativa a personas físicas identificadas o identificables.

Los datos de carácter personal que tengan que ser incluidas en los certificados y en el mecanismo indicado de comprobación del estado de los certificados son considerados datos personales de carácter público a los efectos de la Ley de Firma Electrónica. En este sentido no serán considerados datos públicos disponibles a terceros:

- Solicitudes de certificados, aprobadas o denegadas, así como toda otra información personal para la expedición y mantenimiento de certificados.
- Claves privadas generadas y/o almacenadas por la Entidad de Certificación.
- Cualquier otro dato de carácter personal que no sea susceptible de consulta, almacenamiento o acceso por terceros.

En cualquier caso, los datos captados por el prestador de servicios de certificación tienen la consideración legal de datos de nivel básico.

Los datos personales de tratan de acuerdo con el artículo 9 de la LOPD y garantizando en todo caso la seguridad de los mismos para evitar alteraciones, pérdidas y accesos no autorizados y de acuerdo con las prescripciones establecidas en el Real Decreto 1720/2007, de 21 de diciembre, que aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.

9.4.3 Datos de carácter personal disponibles a terceros

Esta información se trata de información personal que se incluye en los certificados y al referido mecanismo de comprobación del estado de los certificados, de acuerdo con la sección 3.1 de este documento.

Esta información, proporcionada en la solicitud de certificados en los términos previstos en el artículo 17.2 de la Ley 59/2003, de la Ley 59/2003, de 19 de diciembre, de firma

electrónica, se incluye en sus certificados y en el mecanismo de comprobación del estado de los certificados.

Estos datos de carácter personal tienen que estar disponibles para terceros por imperativo legal (“datos públicos”).

En todo caso, se considera no confidencial la siguiente información:

a. Los certificados emitidos o en trámite de emisión.
b. La sujeción de suscriptor a un certificado emitido por la Entidad de Certificación.
c. El nombre y los apellidos del suscriptor del certificado, así como cualquier otra circunstancia o dato personal del titular en el supuesto de que sean significativos en función de la finalidad del certificado, de acuerdo cn este documento.
d. La dirección electrónica del suscriptor del certificado.
e. Los usos y límites económicos reseñados en el certificado.
f. El periodo de validez del certificado, así como la fecha de emisión del certificado y la fecha de caducidad.
g. El número de serie del certificado.
h. Los diferentes estados o situaciones del certificado y la fecha de inicio de cada uno de ellos, en concreto: pendiente de generación y/o entrega, válido, revocado, suspendido o caducado y el motivo que provocó el cambio de estado.
i. Las listas de revocación de certificados (LRCs), así como la resta de informaciones de estado de revocación.
j. La información contenida en la parte pública del Registro de la Entidad de Certificación.

9.4.4 Responsabilidad correspondiente a la protección de los datos personales

La EC-ACC, como mínimo, garantiza el cumplimento de sus obligaciones legales como prestador de servicios de certificación, de conformidad con la Ley 59/2003, de 19 de diciembre, de firma electrónica. Y en virtud de ello, y de acuerdo con el artículo 22 de dicha Ley, responderá por los daños y perjuicios que cause en el ejercicio de la actividad que le es propia, en el caso de incumplir, en lo que aquí interesa, las obligaciones contenidas en el artículo 17 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, relativas a la protección de datos personales.

9.4.5 Gestión de incidencias relacionadas con los datos de carácter personal

El Consorci AOC incluye en este documento su procedimiento de notificación, gestión y respuesta ante las incidencias relacionadas con los datos personales.

Este procedimiento de notificación se inicia cuando el administrador de los sistemas de la Entidad de Certificación, en sus instalaciones, comunica inmediatamente por teléfono con el Responsable de la Entidad de Certificación, describiendo el tipo de incidencia y los efectos que se observan.

Si durante la gestión de la incidencia es necesario hacer modificaciones en el programario o en la configuración de los sistemas, o hay que restaurar copias de seguridad u otras intervenciones parecidas, el administrador se espera a recibir la petición correspondiente por correo electrónico firmado digitalmente, que lo envía el Responsable de la Entidad de Certificación o el responsable técnico del proyecto afectado (en este caso, con copia del mensaje al Responsable de la Entidad de Certificación).

Una vez hechas las actuaciones necesarias y restablecido el normal funcionamiento de los sistemas, el administrador de los sistemas envía por correo electrónico dirigido al Responsable de la Entidad de Certificación un informe descriptivo, que en el caso de las incidencias producidas sobre ficheros que contienen datos de carácter personal, no es más que el formulario tipo debidamente rellenado.

El Responsable de la Entidad de Certificación mantiene copia de los formularios correspondientes a las incidencias registradas durante los 12 últimos meses sobre los ficheros que contienen datos de carácter personal. Estos se guardan en un directorio dedicado dentro del servidor que comparten los usuarios de la Entidad de Certificación, protegido convenientemente para que sólo pueda acceder el personal autorizado; así queda garantizado que se hacen copias de seguridad de su contenido.

En el formulario de Registro de Incidencias se hacen constar los siguientes datos:

- Qué recurso tiene la incidencia.
- Su código y descripción.
- El día y la hora.
- El tipo de incidencia.
- Los efectos.
- El comunicante y el destinatario.
- La respuesta.
- Los procedimientos previstos a realizar.
- La persona que los realizará.
- El procedimiento para la recuperación.
- La persona (y autorización) para la recuperación.
- Los datos restaurados.

9.4.6 Prestación del consentimiento en el uso de los datos personales

Para la prestación del servicio, la EC-ACC necesita recoger y almacenar ciertas informaciones, que incluyen informaciones personales.

En los certificados de clase 1, estos datos son comunicados por los suscriptores, sin necesidad de consentimiento de los afectados poseedores de claves, de acuerdo con lo establecido por la normativa reguladora de la relación del personal al servicio del suscriptor del certificado u otra normativa que resulte aplicable, como prevé el artículo 6 LOPD.

La EC-ACC informa, en todo caso, a los poseedores de claves de la obtención de sus datos personales.

9.4.7 Comunicación de datos personales

El Consorci AOC sólo comunica los datos de carácter personal a terceros en los casos legalmente previstos.

En concreto, el Consorci AOC está obligada a revelar la identidad de los firmantes cuando lo soliciten los órganos judiciales en el ejercicio de las funciones que tengan atribuidas en la resta de supuestos previstos en el artículo 11.2 LOPD.

El Consorci AOC da cumplimiento a todas las prescripciones legales, de conformidad con la política de protección de datos prevista en la sección 9.4.1.

Excepcionalmente y por la situación prevista en la Política General de Certificación, que contempla el caso de finalización de la Entidad de Certificación, el Consorci AOC cederá los datos personales para el supuesto de transferencia de prestación del servicio.

9.5 Derechos de propiedad intelectual

9.5.1 Propiedad de los certificados e información de revocación

La EC-ACC es la única entidad que disfruta de los derechos de propiedad intelectual sobre los certificados que emita.

La EC-ACC concede licencia no exclusiva para reproducir, distribuir, verificar y utilizar los certificados, sin ningún coste, en relación con firmas digitales y/o sistemas de cifrado dentro del ámbito de aplicación de la presente DPC, de acuerdo con el correspondiente instrumento vinculante entre la EC-ACC y la parte que reproduzca y/o distribuya el certificado.

Las anteriores normas figuran en los instrumentos jurídicos que existen entre la EC-ACC y los suscriptores y los verificadores.

Adicionalmente, los certificados emitidos por la EC-ACC contienen un aviso legal relativo a la propiedad de éstos. Esta normativa resulta igualmente de aplicación en el uso de información de revocación de certificados.

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

El Consorci AOC es la única entidad que disfruta de los derechos de propiedad intelectual sobre la política de certificación de la jerarquía pública de certificación de Catalunya.

La EC-ACC es propietaria de la presente DPC.

9.5.3 Propiedad de la información relativa a nombres

El suscriptor (o el poseedor de claves, si procede) conserva cualquier derecho, de existir este, relativo a la marca, producto o nombre comercial contenido en el certificado.

El suscriptor (o el poseedor de claves, si procede) es el dueño del nombre distinguido del certificado, formado por las informaciones especificadas en la sección 3.1 de la presente DPC.

9.5.4 Propiedad de claves

Los pares de claves son propiedad de los suscriptores de los certificados.

Cuando una clave se encuentre fraccionada en partes, todas las partes de la clave son propiedad del propietario de la clave.

9.6 Obligaciones y responsabilidad civil

9.6.1 EC-ACC

9.6.1.1 Obligaciones y otros compromisos

La EC-ACC se obliga a cumplir lo siguiente:

- Determina la comunidad de suscriptores y verificadores de la EC-ACC.
- Aprueba las políticas de certificación i, si procede, les políticas especificas de certificación.
- Aprueba, si procede, este documento, la documentación contractual y reguladora de los servicios de certificación en la comunidad de usuarios de la EC-ACC
- Informa puntualmente al Consorci AOC de todas las informaciones relativas a los cambios a realizar, incidencias en el servicio, reclamaciones, denuncias e inspecciones del servicio.
- Garantiza, bajo su plena responsabilidad, que cumple con todos los requisitos establecidos en la presente DPC.
- Es la única entidad responsable del cumplimiento de los procedimientos descritos en la presente DPC, incluso cuando una parte o la totalidad de las operaciones sean subcontratadas externamente.
- Presta sus servicios de certificación de acuerdo con la presente DPC, donde se detallan, al menos, los contenidos previstos en el artículo 19 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.
- Antes de la emisión y entrega del certificado, la EC-ACC informa de los aspectos previstos en el artículo 18. b) de la Ley 59/2003, de 19 de diciembre, de firma electrónica, así como de los siguientes aspectos:
    - Indicación de la política aplicable, con indicación de que los certificados no se expiden al público y de la necesidad de utilización de dispositivo seguro de creación de firma.
    - Forma en que se garantiza la responsabilidad patrimonial de la EC-ACC.
    - La EC-ACC se declara acorde con la política de certificación, la certificación del prestador de servicios de certificación y la certificación de los productos de firma electrónica utilizados.

  Este requisito se cumple mediante un “Texto divulgativo de la política de certificado” aplicable, que se transmite electrónicamente, utilizando un medio de comunicación duradero en el tiempo, y en lenguaje comprensible.

- La EC-ACC obliga a los suscriptores, poseedores de claves y a los verificadores mediante instrumentos jurídicos apropiados en cada situación, los cuales se transmiten electrónicamente, en lenguaje escrito y comprensible, teniendo en cuenta los siguientes contenidos mínimos:
    - Prescripciones para dar cumplimiento a lo establecido en la presente DPC.
    - Indicación de la política aplicable, con indicación de si los certificados se expiden al público y de la necesidad de uso del dispositivo seguro de creación de firma.
    - Manifestación que la información contenida en el certificado es correcta, excepto notificación en contra por el suscriptor.
    - Consentimiento para la publicación del certificado en el depósito y acceso por terceros a lo mismo.
    - Consentimiento para el almacenaje de la información utilizada para el registro del suscriptor y del poseedor de claves, para la provisión del dispositivo seguro de creación de firma y para la cesión de la mencionada información en terceros, en caso de fin de operaciones de la EC-ACC sin revocación de certificados válidos.
    - Límites de uso del certificado, incluyendo las establecidas en la sección 4.5 de la presente DPC.
    - Información sobre cómo validar un certificado, incluyendo el requisito de comprobar el estado del certificado, y las condiciones en las cuales se puede confiar razonablemente en el certificado, que resulta aplicable cuando el suscriptor actúa como verificador.
    - Limitaciones de responsabilidad aplicables, incluyendo los usos por los cuales la EC-ACC acepta o excluye su responsabilidad.
    - Procedimientos aplicables de resolución de disputas.
    - Ley aplicable y jurisdicción competente.
- La EC-ACC identifica al poseedor de claves, de acuerdo con los artículos 12 y 13 de la Ley 59/2003, de 19 de diciembre, de firma electrónica y la presente DPC. Especialmente, la EC-ACC, comprueba por sí misma la identidad y cualesquiera otras circunstancias personales de los solicitantes de los certificados, de acuerdo con lo establecido en el artículo 13 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

9.6.1.2 Garantías ofrecidas

Garantías ofrecidas a los suscriptores

La EC-ACC garantiza al suscriptor, como mínimo:

El cumplimiento de sus obligaciones legales como prestador de servicios de certificación, de acuerdo con la Ley 59/2003, de 19 de diciembre.

Que no hay errores en las informaciones contenidas en los certificados, conocidos o realizados por la ésta, ni debidos a la falta de diligencia en la gestión de la solicitud de certificado o a la creación de éste.

Que los certificados cumplen todos los requisitos materiales establecidos en la DPC.

Que los servicios de revocación y el uso del Depósito cumplen todos los requisitos materiales establecidos en la DPC.

a) Que, en caso de que haya generado las claves privadas, se mantiene la confidencialidad durante el proceso.

b) La responsabilidad de la EC-ACC, con los límites que se establezcan.

Garantías ofrecidas a los verificadores

La EC-ACC, como mínimo, garantiza al verificador:

a. El cumplimiento de sus obligaciones legales como prestador de servicios de certificación, de acuerdo con la Ley 59/2003, de 19 de diciembre, de firma electrónica.

b. Que la información contenida o incorporada por referencia en el certificado es correcta, excepto cuando indique expresamente lo contrario.

c. En caso de certificados publicados en el directorio, que el certificado ha sido emitido al suscriptor identificado en éste y que el certificado ha sido aceptado, de acuerdo con la sección 4.4 de la presente DPC.

d. Que en la aprobación de la solicitud de certificado y en la emisión del certificado se han cumplido todos los requisitos materiales establecidos en la presente DPC.

e. La rapidez y seguridad en la prestación de los servicios, en especial de los servicios de revocación y directorio.

f. Que los certificados cumplan todos los requisitos materiales establecidos en la presente DPC.

g. Que, en caso de que haya generado las claves privadas, se mantiene la confidencialidad durante el proceso.

h. Que los servicios de revocación y el uso del directorio cumplen todos los requisitos materiales establecidos en la presente DPC.

i. La responsabilidad de la EC-ACC, con los límites que se establezcan.

9.6.2 Entidades de Registro

9.6.2.1 Obligaciones y otros compromisos

Entidades de Registro

La Entidad de Registro se obliga a cumplir lo siguiente:

a. Actúa exclusivamente en relación con personas vinculadas a la Entidad de Registro.

b. Nombra como operador de la autoridad de registro, a uno o más de sus trabajadores, y comunica al Consorci AOClos datos correspondientes a estas personas para la emisión de los certificados de operador correspondiente. Cuando un operador deja de tener capacidad para actuar como lo que es, bajo el control y la autoridad de la Entidad de Registro, esta Entidad solicita de forma inmediata a la EC-ACC la revocación del certificado de operador correspondiente.

c. Valida y aprueba las solicitudes de certificados y acto seguido, genera las tarjetas para los poseedores de claves, de acuerdo con los procedimientos e instrumentos técnicos establecidos por la EC-ACC, de acuerdo con la presente DPC y su documentación de operaciones.

d. Si la Entidad de Registro Interna no dispone de información actualizada del poseedor de claves, comprueba la identidad personalmente o de acuerdo con lo establecido en el artículo 13.4 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, registra un justificante acreditativo del nombre completo, lugar y fecha de nacimiento, DNI y/o cualquier otra información que pueda ser utilizada para diferenciar a una persona respecto de otra en el ámbito de la Entidad de Registro Interna.

e. Verifica, cuando sea necesario, cualquier atributo específico del poseedor de claves, y registra un justificante acreditativo de la información.

f. Realiza o tramita las solicitudes de suspensión, habilitación, revocación y renovación de certificados, de acuerdo con los procedimientos y los instrumentos técnicos establecidos por la EC-ACC, de acuerdo con la presente DPC, y su documentación de operaciones.

g. Almacena los registros, ya sea en papel o de forma electrónica, con las adecuadas medidas de seguridad, autenticidad, integridad y conservación, relativas a la información contenida en el certificado, durante un periodo de 15 años. Estos registros están a disposición de la EC-ACC.

9.6.3 Suscriptores

9.6.3.1 Obligaciones y otros compromisos

Requisitos para todos los tipos de certificados

La EC-ACC obliga al suscriptor de los certificados a:

a. Facilitar a la EC-ACC la información completa y adecuada, conforme a los requerimientos de esta DPC, en especial en lo referente al procedimiento de registro.

b. Manifestar su consentimiento previo a la emisión y entrega de un certificado.

c. Cumplir las obligaciones que se establecen para el suscriptor en la presente DPC y en el artículo 23.1 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

d. Utilizar el certificado de acuerdo con lo establecido en la sección 1.4 de la presente DPC.

e. Notificar a la EC-ACC, sin retrasos injustificables, la pérdida, la alteración, el uso no autorizado, el robo o el compromiso de su dispositivo seguro de creación de firma.

f. Notificar a la EC-ACC, y cualquier persona que el suscriptor crea que pueda confiar en el certificado, sin retrasos injustificables:

    a La pérdida, el robo o el compromiso potencial de su clave privada.

b La pérdida de control sobre su clave privada, a causa del compromiso de los datos de activación (por ejemplo, el código PIN del dispositivo seguro de creación de firma) o por cualquier otra causa.

c Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.

g. Dejar de utilizar la clave privada una vez transcurrido el periodo indicado en la sección correspondiente.

h. Transferir a los poseedores de claves las obligaciones específicas de éstos.

i. No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de la Jerarquía del Consorci AOC, sin permiso previo por escrito.

j. No comprometer intencionadamente la seguridad de la Jerarquía del Consorci AOC.

9.6.3.2 Garantías ofrecidas por el suscriptor

La EC-ACC obliga, mediante el correspondiente instrumento jurídico, al suscriptor a garantizar que:

a. Todas las manifestaciones realizadas en la solicitud son correctas.

b. Todas las informaciones suministradas por el suscriptor que se encuentre contenidas en el certificado son correctas.

c. El certificado se utiliza exclusivamente para usos legales y autorizados, de acuerdo con la presente DPC.

d. Cada firma digital creada con la clave privada correspondiente a la clave pública listada en el certificado es la firma digital del suscriptor y que el certificado ha sido aceptado y se encuentra operativo (no ha expirado ni ha sido revocado) en el momento de creación de la firma.

e. El suscriptor es una entidad final y no una Entidad de Certificación, y no utiliza la clave privada correspondiente a la clave pública lista en el certificado para firmar ningún certificado (o cualquier otro formato de clave pública certificada), ni LRC.

f. Ninguna persona no autorizada ha tenido nunca acceso a la clave privada del suscriptor.

9.6.3.3 Protección de la clave privada

La EC-ACC se obliga, mediante el correspondiente instrumento jurídico, a garantizar que es el único responsable de los daños causados por su incumplimiento del deber de proteger la clave privada.

9.6.4 Verificadores

9.6.4.1 Obligaciones y otros compromisos

La EC-ACC obliga al usuario de certificados a:

a. Asesorarse sobre el hecho que el certificado es apropiado para el uso que se pretende.

b. Verificar la validez, suspensión o revocación de los certificados emitidos, para lo que utilizará información sobre el estado de los certificados.

c. Verificar todos los certificados de la jerarquía de certificados, antes de confiar en la firma digital o en alguno de los certificados de la jerarquía.

d. Tener presente cualquier limitación en el uso del certificado, con independencia de que se encuentre en el mismo certificado o en el contrato de verificador.

e. Tener presente cualquier precaución establecida en un contrato o en otro instrumento, con independencia de su naturaleza jurídica.

f. No monitorizar, manipular o realizar actos de ingeniería inversa sobre la implantación técnica de la jerarquía pública de certificación de Catalunya, sin permiso previo por escrito.

g. No comprometer intencionadamente la seguridad de la jerarquía pública de certificación de Catalunya.

h. Reconocer que las firmas electrónicas producidas por certificados reconocidos de firma reconocida, son firmas electrónicas equivalentes a firmas escritas, de acuerdo con el artículo 3.4 de la Ley 59/2003, de 19 de diciembre.

9.6.4.2 Garantías ofrecidas por el verificador

La EC-ACC obliga al verificador, mediante el correspondiente instrumento jurídico, a manifestar que:

a. Dispone de suficiente información para tomar una decisión informada para confiar o no en el certificado.

b. Es el único responsable de confiar o no en la información contenida en el certificado.

c. Será el único responsable si incumple sus obligaciones como verificador.

9.6.5 Consorci AOC

9.6.5.1 Obligaciones y compromisos

El Consorci AOC tiene las obligaciones siguientes:

a. Operar la EC-ACC, Entidad de certificación raíz de la jerarquía pública de certificación de Cataluña, de manera diligente, de conformidad con las políticas, prácticas y normativa de dicha jerarquía.

b. Operar sus Entidades de Certificación Vinculadas, propias o que presten servicios a las Entidades de Certificación Virtuales, de acuerdo con lo dispuesto en la Política General de Certificación.

c. Garantizar la equivalencia de la seguridad de la operación de las Entidades de Certificación Vinculadas de terceros prestadores de servicios de certificación, y especialmente, velar porque éstos cumplan con las obligaciones previstas en la Política General de Certificación.

9.6.5.2 Garantías ofrecidas a los suscriptores

El Consorci AOC garantiza que la clave privada de la EC-ACC no ha sido comprometida, salvo que así lo indique expresamente mediante el Directorio del Consorci AOC.

El Consorci AOC únicamente garantiza:

a. Que los certificados contienen toda la información exigida por la Ley 59/2003, de 19 de diciembre, de firma electrónica.

b. Que no ha originado ni introducido declaraciones falsas o erróneas en la información de los certificados, ni tampoco ha dejado de incluir información necesaria aportada por la EC-ACC y validada por el Consorci AOC o la Entidad de Registro, en el momento de emisión de los certificados.

c. Que todos los certificados emitidos cumplen los requisitos formales y de contenido.

El Consorci AOC está vinculada a los procedimientos operativos y de seguridad descritos en la presente DPC.

9.6.5.3 Garantías ofrecidas a los verificadores

La responsabilidad del Consorci AOC, que deriva de una relación indirecta, es la prevista en el artículo 23.4 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

9.6.5.4 Exclusión de garantías

El Consorci AOC no garantiza ningún software utilizado por el suscriptor o por cualquier otra persona, para generar, verificar o no utilizar de forma diferente ninguna firma digital o certificado digital emitido por el Consorci AOC, a excepción de los casos en que haya una declaración escrita del Consorci AOC en sentido contrario.

9.6.6 Directorio

9.6.6.1 Obligaciones y compromisos

La EC-ACC puede delegar algunas funciones en el directorio, que en este caso está obligado a su cumplimiento, en las mismas condiciones que ésta.

Las funciones, obligaciones y deberes del directorio se establecen detalladamente en la presente DPC, así como en la documentación jurídica auxiliar, especialmente la entregada a suscriptores, poseedores de claves y verificadores.

9.6.6.2 Garantías

La EC-ACC establece en la presente DPC la responsabilidad civil del directorio, cuando sea operado por una tercera entidad.

9.7 Renuncias de garantías

9.7.1 Rechazo de garantías de la EC-ACC

La EC-ACC 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-ACC

La EC-ACC 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-ACC 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-ACC 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-ACC 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-ACC 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

La EC-ACC establece, en sus instrumentos jurídicos con los suscriptores y los verificadores, cláusulas de supervivencia, en virtud de la que ciertas reglas continúan vigentes después de la finalización de la relación jurídica reguladora del servicio entre las partes.

A este efecto, la EC-ACC vela porque, al menos los requisitos contenidos en las secciones Obligaciones, Responsabilidad civil, Auditoría de conformidad y Confidencialidad, continúen vigentes después de la finalización de la política de certificación y de los instrumentos jurídicos que vinculen la EC-ACC con suscriptores y verificadores.

El Consorci AOC determinará un Plan de Continuidad de Negocio. Este Plan de Continuidad de Negocio establecerá las obligaciones que asume el Consorci AOC en caso de cesación de actividades, dirigidas a mantener en vigencia los certificados emitidos hasta su expiración y el uso y custodia de toda la información generada por el Consorci AOC en su actividad de prestador de servicios de certificación, como por ejemplo, las copias de seguridad, logs y documentos de todo tipo, independientemente del soporte en el que han sido generados o almacenados. A tal efecto, el Consorci AOC se asegura de que se genera una copia de seguridad con periodicidad, como previsión complementaria de la actividad corriente e igualmente del aseguramiento de la continuidad de negocio.

9.11 Notificaciones

La EC-ACC establece, en sus instrumentos jurídicos vinculantes con suscriptores y verificadores, cláusulas de notificación, en las que se establece el procedimiento por el que las partes se notifican hechos mutuamente.

9.12 Modificaciones

9.12.1 Procedimiento para las modificaciones

La EC-ACC puede modificar, de forma unilateral, la presente DPC, siempre que proceda según el siguiente procedimiento:

- La modificación tiene que estar justificada desde el punto de vista técnico, legal o comercial.

- La modificación propuesta por la EC-ACC no puede ir en contra de la política de certificación establecida por el Consorci AOC.

- Se establece un control de modificaciones, para garantizar, en todo caso, que las especificaciones resultantes cumplan los requisitos que se intentan cumplir y que dieron pie al cambio.

- Se establecen las implicaciones que el cambio de especificaciones tiene sobre el usuario, y se prevé la necesidad de notificarle dichas modificaciones.

- La nueva política tiene que ser aprobada por el Consorci AOC.

9.12.2 Periodo y mecanismos para notificaciones

Las modificaciones de la presente DPC se notifican al Consorci AOC, para su posterior aprobación.

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

La EC-ACC establece, en sus instrumentos jurídicos con suscriptores y verificadores, los procedimientos de mediación y resolución de conflictos aplicables.

Con esta finalidad, se tiene en cuenta la consideración como Administración Pública de la EC-ACC.

Las situaciones de discrepancia que se deriven del uso de los certificados emitidos por la EC-ACC, se resuelven aplicando los mismos criterios de competencia que en los casos de los documentos firmados por escrito.

9.13.2 Jurisdicción competente

La EC-ACC establece, en sus instrumentos jurídicos vinculantes con suscriptores y verificadores, una cláusula de jurisdicción competente, indicando que la competencia judicial internacional corresponde a los jueces españoles.

La competencia territorial y funcional se determina en virtud de las reglas de derecho internacional privado y reglas de derecho procesal que resulten de aplicación.

Asimismo, se tiene en cuenta la legislación administrativa que resulte aplicable.

9.14 Ley aplicable

La EC-ACC establece, en sus instrumentos jurídicos con suscriptores y verificadores, que la ley aplicable a la prestación de los servicios, incluyendo la política y prácticas de certificación es la siguiente:

- En general, la ley española, siempre y cuando la EC-ACC siga establecida en el Estado Español, y/o sus servicios de certificación se presten por medio de un establecimiento permanente situado en el Estado Español.
- Y la normativa administrativa correspondiente, estatal y autonómica.

9.15 Conformidad con la ley aplicable

La EC-ACCmanifiesta, 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

La EC-ACC establece, en sus instrumentos jurídicos vinculantes con suscriptores y verificadores, cláusulas de acuerdo íntegro, en virtud de las que se entiende que el instrumento jurídico regulador del servicio contiene la voluntad completa y todos los acuerdos entre las partes.

9.16.2 Subrogación

Los derechos y los deberes asociados a la condición de Entidad de Certificación no pueden ser objeto de cesión a terceros de ningún tipo, ni ninguna tercera entidad puede subrogarse en la posición jurídica de una Entidad de Certificación.

En caso de producirse una cesión o subrogación, se procede a la finalización de dicha Entidad de Certificación.

9.16.3 Divisibilidad

La EC-ACC establececlásulas de divisibilidad, en sus instrumentos jurídicos vinculantes con suscriptores y verificadores, en virtud de las cuales la invalidez de una cláusula no afecta al resto del contrato.

Para el caso que, como causa en los artículos 7 y 8 de la Ley 7/1998 sobre condiciones generales de la contratación, se considerasen no incorporadas al contrato, o nulas algunas o cualquiera de las cláusulas indicadas, la referida no incorporación o nulidad no determina la ineficacia total del contrato, si éste pudiera subsistir sin las cláusulas indicadas.

9.16.4 Aplicaciones

Sin estipulación adicional.

9.16.5 Otras cláusulas

Sin estipulación adicional.

ANEXO – Control documental

Control de versiones DPC EC-ACC 1er semestre 2016

Proyecto:	**Informe modificación del documento DPC EC-ACC**
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	Totes	Revisión global del documento – Integración de CATCert en Consorci AOC	Servei de Certificació Digital AOC	**05/08/2016**