Consorci
Administració Oberta
de Catalunya

Declaración de Prácticas de Certificación
Entidad de Certificación Ciutadania
(EC-CIUTADANIA)

Referencia:	D1111_E0650_N-DPC EC-CIUTADANIA
Versión:	2.0
Fecha:	09/05/2018

Índex

1. Introducción

1.1. Presentación

1.1.1. Tipos y clases de certificados

El Consorci AOC ha definido una tipología de servicios de certificación que permiten, a EC-CIUTADANIA, emitir certificados digitales para varios usos y usuarios finales diferentes.

- Certificados personales, caracterizados por el hecho que el poseedor de la clave privada es una persona física, que actúa en nombre y representación del Suscriptor o titular del certificado (que puede ser él mismo o una persona jurídica a la cual esté vinculado)

Por otro lado, los certificados de empleado público son certificados corporativos, caracterizados por el hecho que el poseedor de la clave privada está vinculado al Suscriptor o titular del certificado, que es una organización del sector público. La persona física poseedora de la clave privada estará identificada en el certificado. Típicamente, EC-CIUTADANIA emite certificados de empleado público por los operadores de la infraestructura (operadores de registro, etc).

El registro de los datos para la emisión de los certificados de empleado público lo realiza la entidad Suscriptora del mencionado certificado, actuando como entidad de registro interna.

El resto de certificados serán certificados de persona vinculada, emitidos en concurrencia con el libre mercado, y habitualmente en régimen de actuación subsidiaria, cuando no existan prestadores que ofrezcan el servicio o el número de los mismos resulte insuficiente para garantizar su distribución efectiva a los usuarios finales (ciudadanos, empresas, profesionales).

El registro de los datos para la emisión de los certificados de persona vinculada lo realiza una entidad de registro, bajo la responsabilidad de la Entidad de Certificación.

El registro de los datos para la emisión de los certificados de persona vinculada lo realiza una entidad de registro, bajo la responsabilidad de la Entidad de Certificación.

1.1.1.1. Certificados personales

EC-CIUTADANIA podrá emitir los siguientes tipos de certificados personales:

- idCAT certificado: es un certificado cualificado en conformidad con aquello establecido a la legislación aplicable, descrita a la sección 9.15 de esta DPC. Garantiza la identidad del Suscriptor y del poseedor de la clave privada de identificación y firma, y permite la generación de la “firma electrónica avanzada”

1.1.1.2. Certificados de pruebas

De cualquiera de los tipos de certificados que recoge la presente política se pueden emitir, en determinadas circunstancias, certificados de pruebas.

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 EC-CIUTADANIA.

EC-CIUTADANIA emite certificados dentro de la jerarquía de certificación operada por el Consorci AOC, por lo 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 EC-CIUTADANIA en la prestación de sus servicios, en cumplimiento de los requisitos establecidos por las políticas que gestiona y la legislación aplicable.

Esta DPC es coherente con aquello establecido en la Política General de Certificación e incluso incluye múltiples referencias en esta, para evitar duplicidades allá donde la DPC no introduce información adicional.

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 EC-CIUTADANIA”.

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

1.3.6.1.4.1.15096.1.2.11

1.2.2. Identificación de políticas de certificación cubiertas por esta DPC

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

Certificados personales:

- **CPISA-2 idCAT** – Certificado de persona física de identificación, y firma electrónica avanzada, emitido por EC-CIUTADANIA. Estos certificados no se podrán emitir a partir de la entrada en vigor de la versión 2.0 de este documento.

  OID: 1.3.6.1.4.1.15096.1.3.1.86.2

- **CPISA-2 idCAT adaptado a eIDAS** (REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la cual se deroga la Directiva 1999/93/CE) – Certificado de persona física de identificación, y firma electrónica avanzada, emitido por EC-CIUTADANIA

  OID: 1.3.6.1.4.1.15096.1.3.2.86.2

Los documentos descriptivos de estos perfiles de certificados se publican en el web del Consorci AOC.

1.3. Comunidad de usuarios de certificados

Esta declaración de prácticas de certificación regula una comunidad de usuarios que obtienen certificados para poder llevar a cabo relaciones administrativas por medios electrónicos, de acuerdo con la ley aplicable y la normativa administrativa correspondiente, que se recogen en el apartado 9.15 Conformidad con la ley aplicable

EC-CIUTADANIA emite certificados idCAT al público, destinados a ciudadanos y ciudadanas catalanes mayores de edad, así como a otras personas (colectivamente llamados Suscriptores) que necesitan relacionarse con las entidades que integran el Sector Público de Cataluña y con otras instituciones.

El certificado idCAT es un certificado cualificado de acuerdo con aquello establecido a la legislación aplicable, descrita a la sección 9.15 de esta DPC.

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 aplicable, descrita a 9.15. Conformidad con la ley aplicable.

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

Conforme a esta función, el Consorci AOC será responsable por la actuación de EC-CIUTADANIA ante los usuarios finales y los terceros verificadores de certificados y firmas electrónicas.

1.3.2. Entidad de Certificación Raíz

El Consorci AOC dispone de una autoridad de certificación principal, que es la raíz de la jerarquía pública de certificación de Cataluña: el EC-ACC, la finalidad de la cual es integrar otras entidades de certificación en el sistema público catalán de certificación mediante la vinculación técnica de las autoridades de certificación correspondientes.

1.3.3. EC-CIUTADANIA

EC-CIUTADANIA es la Entidad de Certificación para dotar de certificados digitales a los ciudadanos y ciudadanas catalanas mayores de edad, así como a otras personas (colectivamente llamados Suscriptores) que necesitan relacionarse con las entidades que integran el Sector Público de Cataluña y con otras instituciones.

EC-CIUTADANIA está vinculada a la jerarquía de entidades de certificación de las entidades públicas de Cataluña y emite los certificados indicados en el punto 1.1.1.

1.3.4. Entidades de Registro

Conforme a aquello establecido a la Política General de Certificación, las Entidades de Registro 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.

El Consorci AOC es responsable del proceso de creación de entidades de registro de EC-CIUTADANIA: exige la formalización del instrumento jurídico pertinente; y verifica que la Entidad de Registro cuenta con los recursos materiales y humanos necesarios; y que ha designado y ha formado al personal que será responsable de la emisión de certificados (los denominados operadores de la entidad de registro). Así mismo, el Consorci AOC es responsable de la emisión de los certificados de operador que estos necesitarán para poder operar (típicamente serán CIPISQ); y validará las peticiones de certificados para operadores de las Entidades de Registro examinando la solicitud y haciendo las comprobaciones necesarias para el cumplimiento de la Política General de Certificación y de esta Declaración de Prácticas de Certificación.

1.3.5. Usuarios finales

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

- Los solicitantes de certificados: son personas mayores de edad que solicitan los certificados. Pueden hacerlo:
    a) Las personas que serán los futuros Suscriptores de los certificados
    b) Otras personas autorizadas - documentalmente – por los futuros Suscriptores (representantes)
- Los Suscriptores o titulares de certificados: para tratarse de certificados individuales personales, son las personas físicas identificadas en el campo “Subject” de los certificados. Tienen licencia de uso del certificado
- Los poseedores de claves: son los Suscriptores de los certificados, en conformidad con aquello establecido en la Política General de Certificación
- Los verificadores de los certificados: son las personas que reciben firmas electrónicas y/o certificados digitales y tienen que verificarlos, como paso previo a confiar en ellos, en conformidad con aquello establecido a la Política General de Certificación

1.4. Uso de los certificados

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

1.4.1. Usos típicos de los certificados

Los certificados idCAT de firma avanzada son certificados cualificados de acuerdo con aquello establecido a la legislación aplicable, tal como se describe a la sección 9.15 de esta DPC, y que dan cumplimiento a aquello dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia TS 101 456.

Los certificados idCAT no funcionan necesariamente con dispositivos cualificados de creación de firma electrónica de acuerdo con dicha legislación aplicable.

Los certificados idCAT garantizan la identidad del Suscriptor, resultando idóneos para ofrecer apoyo a la firma electrónica avanzada.

Aunque la firma electrónica avanzada no se equipara directamente a la firma escrita, esta equiparación se puede producir igualmente en virtud de un contrato de firma electrónica o de una norma jurídica específica (por ejemplo la "ORDEN HACHE/1181/2003, de 12 de mayo, por la que se establecen normas específicas sobre el uso de la firma electrónica en las relaciones tributarias por medios electrónicos, informáticos y telemáticos con la Agencia Estatal de Administración Tributaria"), que establecerá las condiciones adicionales necesarias porque se produzca esta equiparación.

Además, se pueden utilizar para varios usos, entre los que se pueden indicar los siguientes:

- Identificación remota, basada en presentación de la credencial
- Autenticación por medios electrónicos ante sistemas de control de acceso

1.4.2. Aplicaciones prohibidas

1.4.2.1. Informaciones para todos los tipos de certificados

Los certificados no se han diseñado, no se pueden destinar y no se autoriza su uso o reventa como equipos de control de situaciones peligrosas o para usos que requieren actuaciones a prueba de errores, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas, o sistemas de control de armamento, donde un error podría directamente comportar la muerte, lesiones personales o daños medioambientales severos.

1.4.2.2. Certificados personales

Los certificados personales emitidos por EC-CIUTADANIA – los perfiles de los cuales se relacionan con el apartado Identificación de políticas de certificación cubiertas por esta DPC – no podrán utilizarse para los fines descritos a la Política General de Certificación, apartado Aplicaciones prohibidas.

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

Domicilio social: Via Laietana, 26 – 08003 Barcelona

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

Web del Consorci AOC: `www.aoc.cat`

Web del Servicio SCD del Consorci AOC:

http://web.aoc.cat/blog/serveis/catcert-er-idcat/

Web del servicio idCAT del Consorci AOC: www.idcat.cat

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 lo/la Responsable del Servicio SCD del Consorci AOC, basándose en los resultados de una auditoría al efecto, realizada por un tercero, bianualmente.

1.5.4. Procedimiento de aprobación

El sistema documental y de organización de EC-CIUTADANIA 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.

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

Conforme a aquello establecido a la Política General de Certificación.

2.2. Publicación de información de EC-CIUTADANIA

Conforme a aquello establecido a la Política General de Certificación.

2.3. Frecuencia de publicación

La información de EC-CIUTADANIA 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 aquello establecido a la sección 9.12.1 Procedimiento para las modificaciones.

Pasados 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 EC-CIUTADANIA, pudiendo ser consultadas por los interesados.

La información de estado de revocación de certificados se publica de acuerdo con aquello establecido a la sección 4.9.7 Frecuencia de emisión de listas de revocación de certificados (CRL's).

2.4. Control de acceso

Conforme a aquello establecido a la Política General de Certificación.

3. Identificación y autenticación

3.1. Gestión de nombres

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

3.1.1. Tipos de nombres

Conforme a aquello establecido a la Política General de Certificación.

3.1.2. Significado de los nombres

Conforme a aquello establecido a la Política General de Certificación.

3.1.3. Utilización de anónimos y pseudónimos

No se pueden utilizar anónimos ni pseudónimos.

3.1.4. Interpretación de formatos de nombres

Sin estipulación adicional.

3.1.5. Unicidad de los nombres

Conforme a aquello establecido a la Política General de Certificación.

3.1.6. Resolución de conflictos relativos a nombre

Conforme a aquello establecido a la Política General de Certificación.

En lo referente al tratamiento de marcas registradas, ver el apartado 9.5.3.

3.2. Validación inicial de la identidad

3.2.1. Prueba de posesión de clave privada

Conforme a aquello establecido a la Política General de Certificación.

3.2.2. Autenticación de la identidad de una organización

3.2.2.1. Entidades de Registro

Conforme a aquello establecido a la Política General de Certificación.

3.2.2.2. Las entidades suscriptoras de certificados

No aplica, puesto que EC-CIUTADANIA no emite certificados corporativos.

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.

La acreditación de la identidad se puede realizar directamente ante las Entidades de Registro, mediante el proceso de pre-validación, en el que el solicitante consigna los datos directamente a los operadores, los cuales las validan, contrastándolos con los documentos originales aportados (NIF, NIE, pasaporte o DNI otros países) y, si son correctos, los introducen en el sistema y proceden a emitir el certificado.

El solicitante también puede consignar sus datos identificativos en la web idCAT del Consorci AOC. Posteriormente, el solicitante se persona ante una Entidad de Registro, que puede ser la más cercana a su domicilio, y presenta la documentación identificativa que ha indicado a la solicitud (NIF, NIE, pasaporte o DNI otros países) a un operador de registro, aportando también, en los casos que sea necesario una fotocopia de este documento y, si lo desea, una copia impresa del formulario de confirmación de datos que le mostró la web al final del proceso de solicitud.

Los documentos identificativos que aporte el solicitante tienen que estar en vigor. Cuando estén en proceso de renovación, tendrá que aportar el resguardo de renovación; y si este no contiene fotografía, podrá completarse la verificación de la identidad utilizando el documento caducado.

El operador de la Entidad de Registro valida, mediante la fotografía, que el documento identificativo aportado pertenece al solicitante; también comprobará que este es mayor de edad.

Seguidamente, se da al titular el documento de comparecencia u hoja de entrega, que incluye los datos de la solicitud del certificado, porque el solicitante lo firme.

El operador comprobará también que la firma que el Suscriptor acaba de realizar en la solicitud de certificado corresponda a la firma que consta en el documento identificativo (NIF, ANIDO, pasaporte o DNI otros países).

Si todas estas comprobaciones son satisfactorias, se valida la solicitud en el sistema informático, enviándola electrónicamente y de forma segura a EC-CIUTADANIA.

3.2.3.1. Necesidad de presencia personal

Conforme a aquello establecido a la Política General de Certificación.

3.2.4. Información no verificada

L' idCAT Certificat inclou informació del Suscriptor no verificada, com l'adreça de correu electrònic d'aquest.

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 ordinaria, como si es posterior a la revocación del certificado a renovar, el proceso a seguir para la renovación de un certificado será el mismo que para la emisión de certificados nuevos: EC-CIUTADANIA 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 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 aquello establecido a la sección 3.2 Validación inicial de la identidad.

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

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

Los ciudadanos que deseen obtener un certificado idCAT pueden visitar la web del servicio idCAT del Consorci AOC o personarse directamente en las oficinas de cualquier de las entidades de registro (Ayuntamientos, Diputaciones, etc.) que ofrecen esta posibilidad, rellenar el formulario de solicitud y seguir las instrucciones que allá se indican.

4.1.1. Legitimación para solicitar la emisión

Conforme a aquello establecido a la Política General de Certificación.

4.1.2. Procedimiento de alta; Responsabilidades

EC-CIUTADANIA, mediante la participación de las Entidades de Registro, se asegura que las solicitudes de certificados son completas, precisas y están debidamente autorizadas.

Una vez que el operador de registro ha comprobado favorablemente la identidad del solicitante, ha verificado la documentación acreditativa presentada por él y este ha firmado el documento de comparecencia, el operador firma la solicitud autorizándola y la remite a EC-CIUTADANIA.

Para las solicitudes rellenadas vía web, previamente a la personación del solicitante ante una Entidad de Registro: si durante el acto de personación el operador de registro detecta algún error en los datos introducidos – al compararlas con la documentación identificativa que se presenta – el operador podrá introducir los cambios que sean necesarios, siempre que quede constancia documentada del origen del cambio; para lo cual pedirá al solicitante que firme un documento de rectificación de datos.

4.2. Procesamiento de la solicitud de certificación

Cuando EC-CIUTADANIA recibe una solicitud de certificado autorizada por una Entidad de Registro, recupera la correspondiente solicitud de la mesa de solicitudes, lo almacena en la estructura de certificados y la firma, completando así la generación del certificado.

4.2.1. Acciones de EC-CIUTADANIA durante el proceso de emisión

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

Para cada solicitud de certificado enviada, EC-CIUTADANIA actuará conforme a aquello establecido al efecto en la Política General de Certificación – apartado 4.3.1 Acciones de la Entidad de Certificación durante los procesos de emisión y renovación.

4.2.2. Comunicación de la emisión al suscriptor

EC-CIUTADANIA comunicará al solicitante la aprobación o denegación de la solicitud de certificado cursada.

En caso de que haya sido aprobada, también comunicará – cuando corresponda - al futuro poseedor de claves, por correo electrónico, que se ha generado el certificado, que se encuentra disponible y la forma de obtenerlo.

Para obtener el certificado, el suscriptor tiene que acceder en la página web que se indica en el correo electrónico mencionado y seguir las instrucciones que este detalla para descargar el certificado.

4.3. Aceptación del certificado

En determinados casos, EC-CIUTADANIA es responsable de crear el par de claves criptográficas de los certificados idCAT Certificado que emite; y siempre es responsable de generar el certificado digital correspondiente.

EC-CIUTADANIA generará la hoja de solicitud de emisión del certificado, porque sea firmado por el futuro poseedor de claves, conforme a aquello establecido a la Política General de Certificación. De forma que, en el mismo acto, quede constancia documentada:

- de su comparecencia
- de la veracidad y corrección de los datos que constan en la solicitud
- de su acreditación mediante documentación identificativa
- que ha sido informado de la política de protección de datos del Consorci AOC en relación a los certificados que emite EC-CIUTADANIA
- de su conformidad con la Declaración de Prácticas de Certificación de EC-CIUTADANIA
- y de su aceptación del certificado que solicita

4.3.1. Responsabilidades de la Entidad de Registro

4.3.1.1. Para Certificados personales

EC-CIUTADANIA delega en las entidades de registro (más concretamente en la figura del responsable de estas entidades de registro) algunas de sus responsabilidades referentes al proceso de entrega y aceptación de los certificados digitales que emite.

Concretamente, el responsable de la entidad de registro tendrá que:

- informar al poseedor de las claves de sus obligaciones y responsabilidades en relación al certificado que le entrega
- recoger del poseedor de las claves el reconocimiento de la aceptación del certificado, mediante la firma de la hoja de solicitud descrita anteriormente
- custodiar durante 15 años un ejemplar de la hoja de solicitud y aceptación del certificado, debidamente firmada por el poseedor de las claves

4.3.2. Conducta que constituye aceptación del certificado

El certificado se acepta mediante la firma, por parte del poseedor de claves, de la hoja de solicitud y aceptación del certificado.

También se considera la posibilidad de aceptar el certificado mediante un mecanismo telemático de activación del certificado.

4.3.3. Publicación del certificado

Conforme a aquello establecido a la Política General de Certificación.

4.3.4. Notificación de la emisión a terceros

No aplicable.

4.4. Uso del par de claves y del certificado

4.4.1. Uso por parte de los poseedores de claves

Conforme a aquello establecido a la Política General de Certificación.

4.4.2. Uso por el tercero que confía en certificados

Conforme a aquello establecido a la Política General de Certificación.

Por otro lado, dado que los usos previstos del certificado idCAT son administrativos (en los cuales el tercero que confía es una entidad pública), cuando el tercer verificador que quiera permitir el uso del idCAT en sus sistemas no sea una de estas entidades, tendrá que firmar un convenio específico de extensión del uso del certificado, que permitirá al Consorci AOC asumir el riesgo correspondiente.

4.5. Renovación de certificados sin renovación de claves

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

4.6. Renovación de certificados con renovación de claves

Conforme a aquello establecido a la Política General de Certificación.

4.7. Renovación telemática

Conforme a aquello establecido a la Política General de Certificación.

4.8. Modificación de certificados

El Suscriptor de un certificado emitido por EC-CIUTADANIA solamente puede modificar los datos de contacto asociadas al certificado que el Consorci AOC utiliza para enviarle información relativa a la gestión de este (como por ejemplo, la dirección de correo electrónico en que quiere recibir los avisos de próxima caducidad del certificado). Pero en ningún caso se puede modificar la información contenida en el certificado; a todos los efectos, la modificación de esta compuerta la revocación y la emisión de un nuevo certificado.

Para poder cambiar los datos de contacto, el poseedor de las claves tiene que solicitarlo a través de la web del servicio idCAT, seleccionando el certificado e introduciendo los datos nuevos.

4.9. Revocación y suspensión de certificados

4.9.1. Causas de revocación de certificados

Conforme a aquello establecido a la Política General de Certificación.

4.9.2. Legitimación para solicitar la revocación

Puede solicitar la revocación de un certificado:

- El Suscriptor a nombre del cual se emitió el certificado
- La Entidad de Registro que intervino en la emisión
- EC-CIUTADANIA

4.9.3. Procedimientos de solicitud de revocación

La solicitud de revocación tiene que incluir la información suficiente para poder identificar razonablemente, en criterio de EC-CIUTADANIA, por un lado el certificado que se solicita revocar y, de la otra, la autenticidad y la autoridad del solicitante. Como mínimo, los datos de contacto del poseedor de claves, número de NIF o de otro documento identificativo aceptado, la fecha y el motivo de la petición, así como el número de serie del certificado.

La solicitud de revocación tiene que ser entregada personalmente, enviada por correo electrónico firmado o por correo postal certificado firmado.

La petición de revocación, con la documentación necesaria, es recogida, registrada y comunicada por la Entidad de Registro. Se comprueba que la documentación sea suficiente y se autentica y autoriza al solicitante.

Si todo es correcto, un operador de registro lleva a cabo la revocación efectiva, mediante la aplicación informática correspondiente. Y a continuación, de forma automática e inmediata, se indica esta revocación en el estado del certificado en la lista de revocaciones.

La solicitud y la documentación adjunta se archivan.

4.9.4. Plazo temporal de solicitud de revocación

Conforme a aquello establecido a la Política General de Certificación.

4.9.5. Plazo máximo de procesamiento de la solicitud de revocación

Conforme a aquello establecido a la Política General de Certificación.

4.9.6. Obligación de consulta de información de revocación de certificados

Conforme a aquello establecido a la Política General de Certificación.

4.9.7. Frecuencia de emisión de listas de certificados revocados (LCRs)

Conforme a aquello establecido a la Política General de Certificación.

4.9.8. Periodo máximo de publicación de LRCs

Conforme a aquello establecido a la Política General de Certificación.

4.9.9. Disponibilidad de servicios de comprobación de estado de certificados

Conforme a aquello establecido a la Política General de Certificación.

4.9.10. Obligación de consulta de servicios de comprobación de estado de certificados

Conforme a aquello establecido a la Política General de Certificación.

4.9.11. Otras formas de información de revocación de certificados

Sin estipulación adicional.

4.9.12. Requerimientos especiales en caso de compromiso de la clave privada

Conforme a aquello establecido a la Política General de Certificación.

4.9.13. Causas de suspensión de certificados

Además de por las causas previstas en la Política General de Certificación, EC-CIUDADANÍA puede suspender un certificado cuando no haya sido descargado desde la web en la cual la EC lo deja a disposición del Suscriptor en un plazo de 90 días, contados desde su fecha de emisión.

También cuando se superen los 10 intentos fallidos de descarga desde esta misma web.

4.9.14. Efecto de la suspensión de certificados

Conforme a aquello establecido a la Política General de Certificación.

4.9.15. Quién puede solicitar la suspensión

Puede solicitar la suspensión de un certificado:

- El Suscriptor a nombre del cual se ha emitido el certificado
- EC-CIUTADANIA
- Un tercer interesado legitimado para actuar en defensa de los intereses del Suscriptor.

4.9.16. Procedimientos de solicitud de suspensión

EC-CIUTADANIA determina a continuación los procedimientos y los mecanismos de acceso a los sistemas de suspensión, informando en todo caso al Suscriptor de acuerdo con aquello previsto en la ley aplicable descrita en el apartado 9.15. Conformidad con la legislación aplicable.

1) En un primer caso, el Suscriptor de un certificado idCAT hace una llamada al teléfono del Centro de Atención al Usuario (CAU) del Consorci AOC. El Suscriptor se identifica ante el operador del CAU indicándole el número del documento identificativo (NIF, NIE, pasaporte o DNI otros países) con el cual solicitó el certificado.

   Para iniciar la suspensión se requiere la siguiente información:.

   - Fecha y hora de la solicitud de la suspensión
   - Identidad del Suscriptor que solicita la suspensión
   - Información de contacto de la entidad que solicita la suspensión
   - Nombre y apellidos del poseedor de claves a quienes se le tiene que suspender el certificado digital

- DNI del poseedor de claves a quienes se le tiene que suspender el certificado digital
- Número de serie (serial number) del certificado digital que se solicita suspender
- Razón detallada de la petición de suspensión
-

2) El operador introduce este número de documento identificativo en la correspondiente aplicación informática y, apareciéndole todos los datos del titular del certificado que puede comprobar con la persona que realizó la llamada, le plantea la pregunta de desafío que el Suscriptor hizo y respondió en el momento de realizar la solicitud del certificado. Si responde correctamente, el operador considera validada la solicitud de suspensión.
3) El titular del certificado recibe un correo electrónico por el cual se le comunica que se ha suspendido su certificado; las pasas a seguir para habilitarlo de nuevo; y que, si no lo habilita en los 120 días siguientes, su certificado será revocado automáticamente.

4.9.17. Periodo máximo de suspensión

Conforme a aquello establecido a la Política General de Certificación.

4.9.18. Habilitación de un certificado suspenso

El Suscriptor o una persona legitimada para solicitar la suspensión, podrá solicitar la habilitación del certificado que permanece suspendido, personándose e identificándose ante una Entidad de Registro y firmando el correspondiente documento de solicitud de habilitación comunicante que se ha extinguido el motivo que provocó la suspensión.

4.10. Servicios de comprobación de estado de certificados

4.10.1. Características de operación de los servicios

Las CLR's se publican a los servidores del Consorci AOC y en las URLs indicadas en los certificados emitidos.

De forma alternativa, los verificadores podrán consultar los certificados publicados en el directorio dEC-CIUTADANIA.

4.10.2. Disponibilidad de los servicios

Conforme a aquello establecido a la Política General de Certificación.

4.10.3. Otras funciones de los servicios

Sin estipulación adicional.

4.11. Finalización de la suscripción

Conforme a aquello establecido a la Política General de Certificación.

4.12. Depósito y recuperación de claves

No se practica.

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

5.1. Controles de seguridad física

Conforme a aquello establecido a la Política General de Certificación.

5.1.1. Localización y construcción de las instalaciones

Conforme a aquello establecido a la Política General de Certificación.

5.1.2. Acceso físico

Conforme a aquello establecido a la Política General de Certificación.

5.1.3. Electricidad y aire acondicionado

Conforme a aquello establecido a la Política General de Certificación.

5.1.4. Exposición al agua

Conforme a aquello establecido a la Política General de Certificación.

5.1.5. Advertencia y protección de incendios

Conforme a aquello establecido a la Política General de Certificación.

5.1.6. Almacenamiento de apoyos

Conforme a aquello establecido a la Política General de Certificación.

5.1.7. Tratamiento de residuos

Conforme a aquello establecido a la Política General de Certificación.

5.1.8. Copia de seguridad fuera de las instalaciones

Conforme a aquello establecido a la Política General de Certificación.

5.2. Controles de procedimientos

EC-CIUTADANIA garantiza que sus sistemas se operan de forma segura y, por eso, establece e implanta procedimientos para las funciones que afectan a la provisión de sus servicios.

El personal al servicio de EC-CIUTADANIA realiza los procedimientos administrativos y de gestión de acuerdo con la política de seguridad de EC-CIUTADANIA. Esta política de seguridad ofrece apoyo a roles con diferentes privilegios.

5.2.1. Funciones fiables

Conforme a aquello establecido a la Política General de Certificación.

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

5.2.2. Nombre de personas por tarea

Conforme a aquello establecido a la Política General de Certificación.

5.2.3. Identificación y autenticación para cada función

Conforme a aquello establecido a la Política General de Certificación.

5.2.4. Roles que requieren separación de tareas

Conforme a aquello establecido a la Política General de Certificación.

5.3. Controles de personal

EC-CIUTADANIA 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 y, fuera del ámbito laboral, en aquello en lo referente a la seguridad de las infraestructuras
- Ser diligente y responsable en el tratamiento, mantenimiento y custodia de los activos de la infraestructura identificados a 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 apoyos de información a niveles de seguridad inferiores
- Se reporta al Responsable de Seguridad, el más bien posible, cualquier incidente que se considere que afecta a la seguridad de la infraestructura o que limite la calidad de servicio
- Se utilizan los activos de la infraestructura para las finalidades que los han sido encomendadas
- Se utilizan los activos de la infraestructura para las finalidades que los han sido encomendadas
- Se exige documentación escrita que marque sus funciones y medidas de seguridad a las que está sometido

- El responsable de seguridad vela porque el punto anterior sea ejecutado, proveyendo a los responsables de área de toda la información que sea 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 afectat per aquesta normativa és:

- el Responsable del Servicio de Certificación Digital
- el Responsable de EC-CIUTADANIA
- el Responsable de Seguridad
- el Responsable de Operaciones
- el Operador de Ceremónias de Claves
- el Equipo técnico de administración, operación y explotación
- los Administradores de la red
- y los Operadores de las Entidades de Registro

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

- quién hace las peticiones de los certificados
- quién hace la aprobación y validación de las peticiones de certificados
- quién hace la generación / personalización de certificados
- quién custodia las claves o tokens criptográficos
- quién custodia las claves o combinaciones de seguridad de acceso a la sala de operaciones
- quién 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

Conforme a aquello establecido a la Política General de Certificación.

5.3.2. Requisitos de formación

Conforme a aquello establecido a la Política General de Certificación.

El Consorci AOC, además, proporciona a todo el personal involucrado en las operaciones de las Entidades de Registro de EC-CIUTADANIA, 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 al personal interno.

5.3.3. Requisitos y frecuencia de actualización formativa

Conforme a aquello establecido a la Política General de Certificación.

5.3.4. Secuencia y frecuencia de rotación laboral

Sin estipulación adicional.

5.3.5. Sanciones por acciones no autorizadas

Conforme a aquello establecido a la Política General de Certificación.

5.3.6. Requisitos de contratación de profesionales

Conforme a aquello establecido a la Política General de Certificación.

5.3.7. Suministro de documentación al personal

Conforme a aquello establecido a la Política General de Certificación.

5.4. Procedimientos de auditoría de seguridad

5.4.1. Tipo de acontecimientos registrados

Conforme a aquello establecido a la Política General de Certificación.

5.4.2. Frecuencia de tratamiento de registros de auditoría

Conforme a aquello establecido a la Política General de Certificación.

5.4.3. Periodo de conservación de registros de auditoría

Conforme a aquello establecido a la Política General de Certificación.

5.4.4. Protección de los registros de auditoría

Conforme a aquello establecido a la Política General de Certificación.

5.4.5. Procedimientos de copias de seguridad

Conforme a aquello establecido a la Política General de Certificación.

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

- Se guardan en armarios ignífugos
- Sólo personas autorizadas disponen de acceso a las copias de seguridad

- Las copias están identificadas
- Si un material ha contenido copias de seguridad (usb,, dvd's...) y se quieren reutilizar, se asegura que los datos que ha contenido sean totalmente borradas, haciendo imposible su recuperación
- Se autoriza expresamente la extracción de las copias de seguridad fuera de la Entidad de Registro, rellenando una ficha al respeto 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

Conforme a aquello establecido a la Política General de Certificación.

5.4.7. Notificación del acontecimiento de auditoría al causante del acontecimiento

Conforme a aquello establecido a la Política General de Certificación.

5.4.8. Análisis de vulnerabilidades

Conforme a aquello establecido a la Política General de Certificación.

5.5. Archivo de informaciones

Conforme a aquello establecido a la Política General de Certificación.

5.5.1. Tipos de eventos registrados

EC-CIUTADANIA guarda registros de todos los acontecimientos que tengan lugar durante el ciclo de vida de un certificado, incluyendo la renovación de este.

EC-CIUTADANIA guarda un registro del siguiente:

Documentos originales:

- Formulario de solicitud de certificados
- Hoja de entrega de Suscriptor de certificados

5.5.2. Tipo de acontecimientos registrados

EC-CIUTADANIA guarda los registros especificados a la sección 5.5.1 durante 15 años, contados desde el momento de expedición del certificado.

5.5.3. Protección del archivo

Conforme a aquello establecido a la Política General de Certificación.

5.5.4. Procedimientos de copia apoyo

Se hacen copias de seguridad de los logs de acceso lógico al sistema operativo de la LRA. Se encarga un técnico de comunicaciones del Consorci AOC.

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 las personalizaciones para el Consorci AOC de las aplicaciones que apoyan a la PKI. Estas copias las guarda el Consorci AOC a sus instalaciones.

5.5.5. Requisitos de sellado de fecha y hora

Conforme a aquello establecido a la Política General de Certificación.

5.5.6. Localización del sistema de archivo

EC-CIUTADANÍA tiene un sistema de almacenamiento de datos de archivo fuera de sus propias instalaciones, así como se especifica a la sección 5.1.8.

5.5.7. Procedimientos de obtención y verificación de información de archivo

Conforme a aquello establecido a la Política General de Certificación.

5.6. Renovación de claves

Los certificados del EC-CIUDADANÍA renovados se comunican a los usuarios finales, mediante su publicación en la página web del Servicio SCD del Consorcio AOC.

5.7. Compromiso de claves y recuperación de desastre

5.7.1. Procedimiento de gestión de incidencias y compromisos

EC-CIUTADANIA 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, EC-CIUTADANIA inicia las gestiones necesarias, según los documentos Plano 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 EC-CIUTADANIA (o plan de recuperación de desastres) considera el compromiso o la sospecha de compromiso de la clave privada de EC-CIUTADANIA como un desastre.

En caso de compromiso, EC-CIUTADANIA:

- 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 EC-CIUTADANIA ya no son válidos

5.7.4. Desastre sobre las instalaciones

EC-CIUTADANIA desarrolla, mantiene, prueba y, si es necesario, ejecuta un plan de emergencia en 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.

EC-CIUTADANIA 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
- Publicación de información de revocación

La base de datos de recuperación de desastres utilizada por EC-CIUTADANIA 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 EC-CIUTADANIA tiene las medidas de seguridad físicas especificadas en el Plan de Seguridad.

5.8. Finalización del servicio

5.8.1. EC-CIUTADANIA

Conforme a aquello establecido en la Política General de Certificació.

En caso de fin del servicio, EC-CIUTADANIA:

- Comunicará el cese de su actividad a las entidades afectadas, con una antelación mínima de dos meses
- Informará a las entidades afectadas sobre el tratamiento de los certificados emitidos que todavía no hayan expirado y, especialmente, sobre el mecanismo de consulta del estado de estos que se ofrecerá

- Transferirá las obligaciones de EC-CIUTADANIA a otras personas jurídicas, bajo su consentimiento

Se prevé que EC-CIUTADANIA transfiera los certificados, en los términos previstos a la legislación aplicable, descrita a la sección 9.15 de esta DPC.

5.8.2. Entidad de Registro

Las Entidades de Registro tendrán que conservar y custodiar diligentemente toda la información generada en su actividad como Entidad de Registro durante 15 años después de finalizar las actividades relacionadas con la Entidad de Registro.

6. Controles de seguridad técnica

EC-CIUTADANIA 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 apoyo.

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

El par de claves podrá ser generado por el futuro poseedor de claves o por la Entidad de Registro.

6.1.1.2. Información para los certificados idCAT CPISA

Las claves pública y privada de los certificados idCAT las puede generar el Consorci AOC y enviarlas al poseedor de claves de forma segura. También pueden ser generadas por el futuro poseedor de claves, quienes remitirá la correspondiente prueba de posesión de clave privada (PKCS#10) a EC-CIUTADANIA.

Estas claves no se almacenan, de forma que, en caso de suspensión, revocación o expiración del certificado, el Consorci AOC no responderá por la pérdida de información que hubiera sido cifrada con ellas.

6.1.2. Envío de la clave privada al Suscriptor

6.1.3. Envío de la clave pública al emisor del certificado

Conforme a aquello establecido a la Política General de Certificación.

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

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

La clave pública de EC-CIUTADANIA se publica en el directorio dEC-CIUTADANIA, en forma de certificado CIC firmado por el EC-ACC. Los usuarios pueden acceder al directorio para obtener las claves públicas de EC-CIUTADANIA.

Este mismo certificado también se publica en la web del Consorci AOC.

Adicionalmente, en aplicaciones S/MIME, el mensaje de datos contiene una cadena de certificados, incluyendo los certificados CIC con las claves públicas de las Entidades de Certificación de la jerarquía (en este caso, de EC-CIUTADANIA y de la EC-ACC) que, de esta forma, son distribuidas a los usuarios.

6.1.5. Medidas de claves

Las claves de EC-CIUTADANIA son de 2.048 bits.

Las claves de todos los certificados emitidos por EC-CIUTADANIA 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

Conforme a aquello establecido a la Política General de Certificación.

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

Conforme a aquello establecido a la Política General de Certificación.

La generación de claves para los certificados idCAT emitidos por EC-CIUTADANIA se realiza mediante aplicaciones informáticas.

6.1.9. Propósitos de uso de claves

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

6.2. Protección de la clave privada

6.2.1. Módulos de protección de la clave privada

6.2.1.1. Estándares de los módulos criptográficos

Conforme a aquello establecido a la Política General de Certificación.

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

Conforme a aquello establecido a la Política General de Certificación.

6.2.3. Depósito de la clave privada

Conforme a aquello establecido a la Política General de Certificación.

6.2.4. Copia de seguridad de la clave privada

Conforme a aquello establecido a la Política General de Certificación.

6.2.5. Archivo de la clave privada

Conforme a aquello establecido a la Política General de Certificación.

6.2.6. Introducción de la clave privada en el módulo criptográfico

Conforme a aquello establecido a la Política General de Certificación.

6.2.7. Almacenamiento de la clave privada en el módulo criptográfico

Conforme a aquello establecido a la Política General de Certificación.

6.2.8. Método de activación de la clave privada

La clave privada del suscriptor se activa mediante la introducción del PIN en la correspondiente aplicación de generación de firma.

Esta aplicación en los sistemas informáticos basados en windows es lo Cryptographic Service Provider. La web del servicio idCAT ofrece la posibilidad, en la sección “antes de hacer la solicitud”, de actualizar el sistema del usuario con esta aplicación, mediante un enlace a la web de Microsoft.

Los sistemas basados en Netscape, pueden utilizar la aplicación PKCS #11.

6.2.9. Método de desactivación de la clave privada

Conforme a aquello establecido a la Política General de Certificación.

6.2.10. Método de destrucción de la clave privada

Conforme a aquello establecido a la Política General de Certificación.

6.2.11. Clasificación de los módulos criptográficos

Los módulos de EC-CIUTADANIA (EJBCA Enterprise) están certificados Common Criteria EAL 4+.

6.3. Otros aspectos de gestión del par de claves

6.3.1. Archivo de la clave pública

EC-CIUTADANIA archiva sus claves públicas, de acuerdo con aquello establecido a la sección 6.2.

6.3.2. Periodos de utilización de las claves pública y privada

Conforme a aquello establecido a la Política General de Certificación.

6.4. Datos de activación

6.4.1. Generación e instalación de los datos de activación

La generación e instalación de los datos de activación se basa en el Cryptographic Service Provider.

6.4.2. Protección de los datos de activación

El usuario es responsable de cuidar su clave privada con una palabra de paso tan completa como sea posible, a través de la aplicación (Cryptographic Service Provider).

Se aconseja que esta palabra de paso no sea demasiado corta y esté formada por números y letras.

El Suscriptor tiene que recordar esta palabra de paso.

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

Conforme a aquello establecido a la Política General de Certificación.

6.5.2. Evaluación del nivel de seguridad informática

La aplicación de autoridad de certificación, mediante la cual opera EC-CIUTADANIA (EJBCA Enterprise), es fiable, dado que obtuvo la certificación Common Criteria EAL 4+.

6.6. Controles técnicos del ciclo de vida

6.6.1. Controles de desarrollo de sistemas

Conforme a aquello establecido a la Política General de Certificación.

6.6.2. Controles de gestión de seguridad

Conforme a aquello establecido a la Política General de Certificación.

Además, EC-CIUTADANIA garantiza que sus funciones de gestión de las operaciones de los módulos criptográficos son suficientemente seguras; en particular, existen instrucciones para:

a) Operar los módulos de forma correcta y segura
b) Instalar los módulos minimizando el riesgo de quiebra de los sistemas
c) Proteger los módulos contra virus y software malicioso, para garantizar la integridad y validez de la información que procesan.

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 en las diferentes redes de EC-CIUTADANIA es limitado a individuos debidamente autorizados. En particular:

- Se implementan controles (cómo por ejemplo cortafuegos) para proteger la red interna de dominios externos accesibles por terceras partes. Los cortafuegos se configuran de forma que se impidan acceso y protocolos que no sean necesarios para la operación de EC-CIUTADANIA.
- Los datos sensibles (incluyendo los datos de registro del Suscriptor) se protegen cuando se intercambian a través de redes no seguras.
- Se garantiza que los componentes locales de red (cómo enrutadors/routers) se encuentran ubicados en entornos seguros; también se garantiza 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

Conforme a aquello establecido a la Política General de Certificación.

Los documentos descriptivos de los varios perfiles de certificados digitales que expide EC-CIUTADANIA se publican en la web del Consorci AOC.

7.2. Perfil de la lista de revocación de certificados

Conforme a aquello establecido a la Política General de Certificación.

8. Auditoría de conformidad

EC-CIUTADANIA 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 Cataluña.

EC-CIUTADANIA puede delegar la ejecución de las auditorías en una tercera entidad contratada por el Consorci AOC. En estos casos, EC-CIUTADANIA coopera completamente con el personal que lleva a cabo la investigación.

8.1. Frecuencia de la auditoría de conformidad

Conforme a aquello establecido a la Política General de Certificación.

8.2. Identificación y calificación del auditor

EC-CIUTADANIA se dirige a auditores independientes externos para la realización de las auditorías anuales de conformidad. Estos tienen que demostrar experiencia en seguridad informática, en seguridad de Sistemas de Información y en auditorías de conformidad de Autoridades de Certificación y de los elementos relacionados.

8.3. Relación del auditor con la entidad auditada

Las auditorías externas de conformidad ejecutadas por terceros son realizadas por entidades independientes de EC-CIUTADANIA.

8.4. Relación de elementos objeto de auditoría

Conforme a aquello establecido a la Política General de Certificación.

8.5. Acciones a emprender como resultado de una falta de conformidad

Conforme a aquello establecido a la Política General de Certificación.

8.6. Tratamiento de los informes de auditoría

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

9. Requisitos comerciales y legales

9.1. Tarifas

9.1.1. Tarifa de emisión o renovación de certificados

El Consorci AOC establece las tarifas que aplica EC-CIUTADANIA en la prestación de sus servicios. Las tarifas se pueden consultar en la web del Consorci AOC.

9.1.2. Tarifa de acceso a certificados

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

9.1.3. Tarifa de acceso a información de estado de certificado

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

9.1.4. Tarifas 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 a la legislación aplicable, descrita a la sección 9.15. Conformidad con la ley aplicable, excepto cuando se encuentre eximida por Ley de esta obligación. Este seguro cubre las actuaciones del Consorci AOC como prestador de servicios de certificación.

9.2.2. Otros activos

Sin estipulación adicional.

9.2.3. Cobertura de aseguramiento para Suscriptores y terceros que confían en certificados

En caso de uso incorrecto o no autorizado de los certificados, el Consorci AOC (o EC-CIUTADANIA) no actuará como agente fiduciario frente a suscriptores y terceras

personas, que tendrán que dirigirse contra el infractor de las condiciones de uso de los certificados establecidas por el Consorci AOC (o EC-CIUTADANIA).

9.3. Confidencialidad

9.3.1. Informaciones confidenciales

Conforme a aquello establecido a la Política General de Certificación.

9.3.2. Informaciones no confidenciales

Conforme a aquello establecido a la Política General de Certificación.

9.3.3. Responsabilidad para la protección de información confidencial

Conforme a aquello establecido a la Política General de Certificación.

9.4. Protección de datos personales

9.4.1. Política de Protección de Datos Personales

Conforme a aquello establecido a la Política General de Certificación.

9.4.2. Datos de carácter personal no disponibles a terceros

Conforme a aquello establecido a la Política General de Certificación.

9.4.3. Datos de carácter personal disponibles a terceros

Conforme a aquello establecido a la Política General de Certificación.

9.4.4. Responsabilidad correspondiente a la protección de datos personales

Conforme a aquello establecido a la Política General de Certificación.

9.4.5. Responsabilidad correspondiente a la protección de datos personales

Conforme a aquello establecido a la Política General de Certificación.

9.4.6. Prestación del consentimiento para el tratamiento de los datos personales

Conforme a aquello establecido a la Política General de Certificación.

9.4.7. Comunicación de datos personales

Conforme a aquello establecido a la Política General de Certificación.

9.5. Derechos de propiedad intelectual

9.5.1. Propiedad de los certificados e información de revocación

Conforme a aquello establecido a la Política General de Certificación.

9.5.2. Propiedad de la Política de Certificación y Declaración de Prácticas de Certificación

Conforme a aquello establecido a la Política General de Certificación.

9.5.3. Propiedad de la información relativa a nombres

Conforme a aquello establecido a la Política General de Certificación.

9.5.4. Propiedad de claves

Conforme a aquello establecido a la Política General de Certificación.

9.6. Obligaciones y responsabilidad civil

9.6.1. Entidades de Certificación

9.6.1.1. Obligaciones generales de EC-CIUTADANIA

Conforme a aquello establecido a la Política General de Certificación.

9.6.1.2. Requisitos específicos para los certificados personales

Conforme a aquello establecido a la Política General de Certificación.

9.6.1.3. Garantías ofrecidas a Suscriptores y verificadores

Conforme a aquello establecido a la Política General de Certificación.

9.6.2. Obligaciones y otros compromisos de las Entidades de Registro

9.6.2.1. Obligaciones y otros compromisos

EC-CIUTADANIA puede delegar algunas funciones a Entidades de Registro que, en este caso, quedan obligadas a su cumplimiento, en iguales condiciones que la Entidad de Certificación.

La Entidad de Registro actúa en su propio nombre, sin perjuicio de la responsabilidad de la EC- CIUTADANIA.

La Entidad de Registro queda obligada a registrar los datos del certificado y su aprobación en caso de ser correctos, así como al registro de los datos de este certificado, por el cual realiza las comprobaciones que considere necesarias en relación a la identidad y el resto de datos personales y complementarias de los suscriptores y, si fuera necesario, de los poseedores de claves.

Estas comprobaciones incluyen la justificación documental aportada por el solicitante y, si la Entidad de Registro lo considerara necesario, cualquiera otro documento e información relevante, facilidades por el suscriptor, por el poseedor de claves o por terceras personas.

Si la Entidad de Registro detectara errores en los datos que están incluidas en los certificados, o en los documentos, que justificaran estos datos, está obligada a realizar los cambios que considere necesarios antes de la emisión del certificado, o a la paralización del proceso de emisión y a gestionar con el suscriptor la incidencia correspondiente.

En caso de que la Entidad de Registro corrija los datos sin gestión previa de la incidencia correspondiente con el suscriptor, queda obligada a notificar los datos que finalmente se certifiquen al suscriptor en el momento de la entrega.

La Entidad de Registro se reserva el derecho a no aprobar la solicitud de emisión del certificado, cuando la justificación documental aportada por el solicitante sea insuficiente para la correcta identificación y/o autenticación del suscriptor.

9.6.3. Garantías ofrecidas a Suscriptor y verificadores

9.6.3.1. Garantía del Consorci AOC para los servicios de certificación digital

Conforme a aquello establecido a la Política General de Certificación.

9.6.3.2. Exclusión de la garantía

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

9.6.4. Suscriptores

9.6.4.1. Obligaciones y otros compromisos

9.6.4.1.1. Informaciones para todos los tipos de certificados

Además de aquello establecido a la Política General de Certificación, EC-CIUTADANIA obliga al Suscriptor a:

1. Utilizar el par de claves exclusivamente para firmas electrónicas y conforme a cualquier otra limitación que le sea notificada.
2. Ser especialmente diligente en la custodia de su clave privada y de su dispositivo cualificado de creación de firma, con el fin de evitar usos no autorizados.
3. El Suscriptor genera sus propias claves, por lo tanto, se obliga a:
    i. Generar sus claves de Suscriptor utilizando un algoritmo cualificado como aceptable para la firma electrónica cualificada.
    ii. Crear las claves dentro del dispositivo cualificado de creación de firma.
    iii. Utilizar longitudes y algoritmos de clave cualificados como aceptables para la firma Electrónica cualificada.
4. Notificar al EC, sin retrasos injustificables, la pérdida, la alteración, el uso no autorizado, el robo o el compromiso de su dispositivo cualificado de creación de firma.

9.6.4.1.2. Informaciones específicas para los certificados de firma electrónica cualificada

No aplica.

9.6.4.2. Garantías ofrecidas por el Suscriptor

Conforme a aquello establecido a la Política General de Certificación.

9.6.4.3. Protección de la clave privada

Conforme a aquello establecido a la Política General de Certificación.

9.6.5. Verificadores

9.6.5.1. Obligaciones y otros compromisos

Conforme a aquello establecido a la Política General de Certificación.

9.6.5.2. Garantías ofrecidas por el verificador

Conforme a aquello establecido a la Política General de Certificación.

9.6.6. Otros participantes

9.6.6.1. Obligaciones y garantías del directorio

Conforme a aquello establecido a la Política General de Certificación.

9.6.6.2. Garantías ofrecidas por el directorio

EC-CIUTADANIA tiene la responsabilidad civil del directorio de certificación.

9.7. Renuncias de garantías

9.7.1. Rechazo de garantías de EC-CIUTADANIA

Conforme a aquello establecido a la Política General de Certificación.

9.8. Limitaciones de responsabilidad

9.8.1. Limitaciones de responsabilidad de EC-CIUTADANIA

Más allá de las limitaciones de los prestadores de servicios de certificación establecidas a la legislación aplicable, descrita en el apartado 9.15. Conformidad con la ley aplicable , EC-CIUTADANIA limita su responsabilidad restringiendo el servicio a la emisión y la gestión de certificados y, en su caso, de pares de claves de suscriptores.

EC-CIUTADANIA limita 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

EC-CIUTADANIA incluye cláusulas para limitar su responsabilidad en caso fortuito y en caso de fuerza mayor, en los instrumentos jurídicos con los Suscriptores.

9.9. Indemnizaciones

9.9.1. Cláusula de indemnización de Suscriptor

No se establecerá cláusula de indemnización del Suscriptor.

9.9.2. Cláusula de indemnización de verificador

No se establecerá cláusula de indemnización del verificador.

9.10. Plazo y finalización

9.10.1. Plazo

EC-CIUTADANIA establece, en sus instrumentos jurídicos con los Suscriptores, una cláusula que determina el periodo de vigencia de la relación jurídica en virtud de la cual los suministra certificados.

9.10.2. Finalización

EC-CIUTADANIA establece, en sus instrumentos jurídicos con los Suscriptores, una cláusula que determina las consecuencias de la finalización de la relación jurídica en virtud de la cual los suministra certificados.

9.10.3. Supervivencia

Conforme a aquello establecido a la Política General de Certificación.

9.11. Notificaciones

Conforme a aquello establecido a la Política General de Certificación.

9.12. Modificaciones

9.12.1. Procedimiento para las modificaciones

Conforme a aquello establecido a la Política General de Certificación.

9.12.2. Plazo y mecanismos para notificaciones

Las modificaciones de este documento serán aprobadas por el Consorci AOC, conforme a aquello que se establece en el apartado 1.5.

9.12.3. Circunstancias en las que un OID tiene que ser cambiado

Sin estipulación adicional.

9.13. Resolución de conflictos

9.13.1. Resolución extrajudicial de conflictos

Conforme a aquello establecido a la Política General de Certificación.

9.13.2. Jurisdicción competente

Conforme a aquello establecido a la Política General de Certificación.

9.14. Ley aplicable

Conforme a aquello establecido a la Política General de Certificación.

9.15. Conformidad con la ley aplicable

Conforme a aquello establecido a la Política General de Certificación.

9.16. Cláusulas diversas

9.16.1. Acuerdo íntegro

Conforme a aquello establecido a la Política General de Certificación.

9.16.2. Subrogación

Conforme a aquello establecido a la Política General de Certificación.

9.16.3. Divisibilidad

Conforme a aquello establecido a la Política General de Certificación.

9.16.4. Aplicaciones

Sin estipulación adicional.

9.16.5. Otras cláusulas

Sin estipulación adicional.

ANEXO – Control documental

Proyecto:	**Informe creación del documento DPC EC-CIUTADANIA**
Entidad de destino:	**Servicio SCD - Consorci AOC**
Código de referencia:	**Revisión 1er semestre 2018**
Versión:	**2.0**
Fecha de la edición:	**09/05/2018**

Versión	Partes que cambian	Descripción del cambio	Autor del cambio	Fecha del cambio
1.0	Todo el documento	Redacción inicial de la Declaración de Prácticas de Certificación de EC-CIUTADANIA	Servicio CATCert del Consorci AOC	18/09/2014
1.1	Todo el documento	Revisión ortográfica del documento	Servei SCD del Consorci AOC	20/01/2016
2.0	Todo el documento	Revisión global para adaptación a eIDAS	Servei SCD del Consorci AOC	09/05/2018